

Applique—Windows-based system for Force XXI.

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

—Guilio Douhet

The Profession of Arms in the Information Age

By ARSENIO T. GUMAHAD II



Many believe information is a potent instrument in war. The military subscribes to this idea and calls it *information warfare*, defined as any actions that deny, exploit, corrupt, or destroy enemy information and its functions; protect us from such actions; and exploit friendly military information functions. To some, information warfare simply means using information to

achieve national objectives—a form of war about who knows what, when, where, and why and just how well we know both ourselves and our enemy. Its target seems to be the human mind. Information dominance has thus become a prerequisite for fighting future wars.

The use of information in war has been a basic warfighting requirement throughout history. Technology has made information more available, and now it may become the weapon of choice. Furthermore, a revolution in military affairs (RMA) involving information may be on the horizon. Some view information warfare only in a supporting role—enhancing traditional combat missions. Others regard it as a powerful capability on the strategic level, at a point on the conflict spectrum before general escalation and deployment of combat forces for action.

In addition, some hold that information warfare can be conducted prior to conflict breaking out. Modern strategy often perceives an enemy state as a system of concentric rings representing fielded armies, the population, infrastructure, organic essentials, and leadership with information binding them together. Disrupting the information flow by attacking internal infrastructure hinders the ability of an enemy to conduct offensive operations. However, some caution that

Lieutenant Colonel Arsenio T. Gumahad II, USAF, serves as a project director within the Office of Space and Technology at Headquarters, Department of the Air Force.

advocates of information warfare ignore its unanticipated and perhaps counterproductive effects.

Information is increasingly becoming important to the power and wealth of modern society. Nations once fought for control of territory and

What is Information?

Information begins as derived data from observable facts or events. Interpreting data leads to the development of information. The ultimate interpreter is the person receiving the data. At times, though, an observed event is too complex for the human mind to dissect. Machines are thus used to reduce data into a manageable and comprehensible set. They are information systems and come in both hardware and software forms. The draft of Joint Pub 3-13, *Information Warfare*, refers to information as any communication or representation of knowledge such as facts, data, or opinions in any medium or form. Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines it as the meaning that a human assigns to data by means of the known convention used in their representation. Others conceive of it as a physical property—like mass and energy, inherent in all matter. Under this concept military systems are seen as being based on, if not composed of, information. The role of information warfare therefore becomes apparent: “If information is a veritably physical property, then in the information age winning wars may depend on being able to hurl the most information at the enemy, while safeguarding against retaliation” (John Arquilla and David Ronfeldt, “Information, Power, and Grand Strategy: In Athena’s Camp,” in *The Information Revolution and National Security: Dimensions and Directions*.)

resources; but the new battleground also involves the information domain. As one characterization of this phenomenon has it:

*Evolving technologies may result in a transition from information in warfare—information as a supporting function of the traditional attrition/maneuver operations—to information as warfare—in which attrition and maneuver become supporting elements of military, political, and economic leverage through information control.*¹

Advanced societies depend on an infrastructure that includes subways, airports, telephone networks, and electric power grids. Terrorists, knowledgeable of these vulnerabilities, need only target them to wreak havoc. The Internet is now a popular and convenient vehicle for terrorists and rogue nations to exchange techniques for producing crude but effective weapons.

Two forms of sabotage or terrorism are possible. The first is the traditional disruption of order using violence. The second and more sophisticated is either electronic or information-based.

The United States relies upon technology and information systems to conduct its affairs. Targeting them creates widespread confusion and terror. In government and industry the threat of intrusion is all too real. According to the National Computer Security Association, 69 percent of those firms surveyed in 1993 were infected with a malicious virus, a problem which costs American business an estimated \$3 billion annually.

The government is not immune to such tampering. An attack on the Internet by a graduate student in 1990 disrupted computer installations nationwide. In the same year Australian hackers were charged with damaging data on U.S. government computers. The pool of potentially hostile information warriors is huge and includes former

the pool of potentially hostile information warriors is huge

Soviet and Warsaw Pact intelligence operatives, mercenaries, unemployed technical experts, et al. Eastern Europe, particularly Bulgaria, is said to be the leading exporter of viruses today.

Law and Morality

The Air Force Chief of Staff, General Ronald Fogleman, suggests that “because exploiting [information systems] will readily cross international borders, we must be cognizant of what the laws allow and will not allow.” Information warfare raises questions that are difficult to address. When does war begin in an electronic environment? How does one measure damage and define victory? Does a malicious probe of a computer system warrant response in kind or a more violent response? Who decides to deploy offensive information weapons? Would a systems attack by the United States require congressional approval?

The vulnerabilities of traditional nonmilitary targets are heightened in information warfare. Since enemy civilian infrastructure is a potential target,

*... infowar may only refine the way modern warfare has shifted toward civilian targets. Taking down a country’s air traffic control or phone systems might be done cleanly with computers—but it still represents an attack on civilians.*²

As in the case of nuclear weapons, Clausewitz’s notion of absolute war appears real in conducting information warfare. While the attack is clean the resulting suffering may be morally unjustifiable. Consideration of moral and legal issues raised by information warfare has not advanced as quickly as technology and doctrine. They span the legal spectrum and include issues of intelligence, space, use of force, and neutrality.

1st Combat Camera Squadron (James D. Mossman)Air operations center,
Roving Sands '97.

Although our military justice system provides a limited foundation on which to base new laws and regulations in this area, the only recourse is to extend the provisions of current laws to cover information warfare. Without a definitive legal basis, however, the limits of this new form of warfare remain vague and controversial.

Cyber Warriors

Equipment for the cyber warrior is not science fiction. Development is underway—partly as advanced demonstrations found in the Army science and technology master plan—and includes multisensor-aided technology, digital battlefield communications, intelligent minefields, precision munitions, night imaging, and integrated multimedia information transport. It is only a matter of time before these systems move from the laboratory to the battlefield. The cyber warrior is almost completely autonomous with tools configured to provide maximum information about the combat environment. As an integrated capability, the gear allows for collecting, processing, analysis, and interpreting information critical to a mission. When Sun Tzu stated that “If you know your enemy and know yourself, you need not fear

the result of a hundred battles” he was referring to what is known today as *situational awareness*.

Hierarchical organizations were a hallmark of the industrial age. The need to respond to the innovations of the industrial revolution produced a hierarchical society. This strong structure was necessary to attain strict organizational harmony and discipline. The military more than any other institution needed strong command structure to prosecute its unique mission of organized violence. It is evident that order and discipline characterize the professional military, especially in combat.

Futurists predict a notable shift in societal behavior in the information age. Some envision conditions in which the individual is the centerpiece—personal autonomy as the common element of future social interaction—a world which becomes “multi-centered and multi-functional.”³ Here “we will socialize in digital neighborhoods in which physical space will be irrelevant and time will play a different role.”⁴ In an address before the Association of the United States Army in 1994 General Frederick Franks stated that “as information proliferates at faster speeds and is available to a wider array of individuals, hierarchical organizations evolve into networks and power is shifted more to individuals and groups.”

The challenge to military leaders will be integrating disparate interests and varied emotional levels of individuals. The traditional collective and corporate nature of armed forces is affected by a trend toward individualism. For armies to succeed in war they must have a cohesive, integrated, and common objective. The military is built around a “team concept” wherein the well-being of the unit supersedes that of the individual. Members functioning strictly as individuals undermine unit integrity and threaten mission success.

With the stroke of a key and access to an e-mail address, one can easily bypass the normal chain. Democratic principles of free speech could damage the effectiveness of established channels if taken to the extreme. (The President has an Internet address so that anyone, anywhere, anytime

conflicts in the information age will not be less common or less violent

can send a message to him, unfiltered and unedited.) But is the chain of command necessary in the information age? Hierarchical organization must endure for the military to succeed in battle. But it is questionable whether the structure of the military will survive if central bureaucracies disappear, and some foresee a day when traditional command and control arrangements will become obsolete. But unity of command— one precept which has remained unaltered in every successful war—must not be compromised. Thus greater discipline is required to preserve command unity and control.

Training and Doctrine

Information technology shapes training. State-of-the-art technology promises to make it more cost-effective without sacrificing performance and perhaps even improving it. Simulators are more realistic and offset the high operational price of real-world training.

*U.S. tank commanders of the 21st century will train in a virtual world more than in the real one. The result will be soldiers who are better prepared—by computer simulators integrated into their vehicles that will enable them to practice just hours before combat.*⁵

The Army is experimenting with battle laboratories using advanced technology and systems to simulate the complex interaction of diverse elements on the future battlefield. An Army exercise conducted in autumn 1994, Atlantic Resolve, employed live, virtual, and constructive simulations for training and experimentation. The method was positive and since then the battle laboratory has paid dividends by conditioning decisions in resource allocation and weapons acquisition.

The high-tech military of the future will be smaller but more sophisticated and specialized. In two to three decades the organizational structure

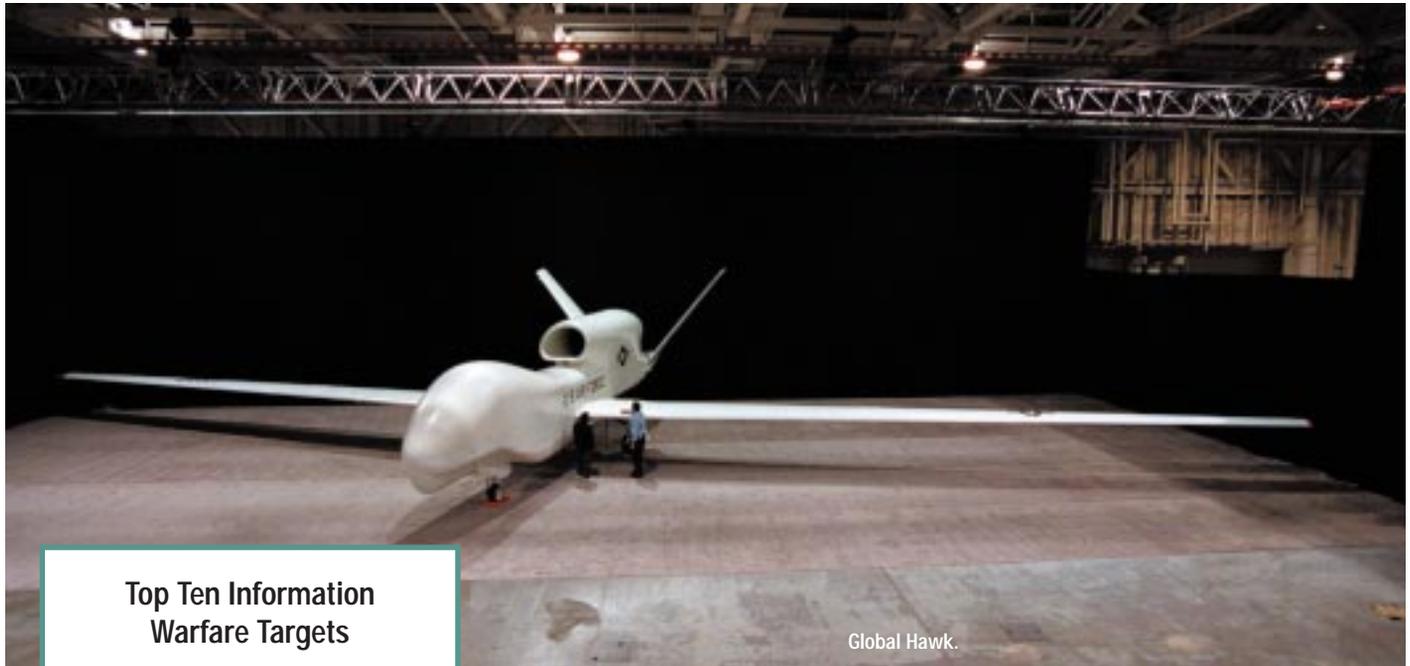
will favor direct lines of command with mid-level grades eliminated. The military will be comprised of well trained, skilled warrior-technicians who are comfortable operating with advanced electronic gadgetry.

Conflicts in the information age will not be less common or less violent. On the contrary, the transition period between the industrial and information ages is likely to be even more chaotic.⁶ If committed to war, cyber warriors will fight as ferociously as their predecessors. Information will enhance the way they operate on the battlefield. These future warriors will quickly outflank and outmaneuver an enemy with knowledge of its position and combat situation. With information age weapons at their disposal they will engage an enemy precisely and decisively.

For information to be a catalyst for a new RMA, doctrinal and organizational changes must occur. Technology enables the application of revolutionary innovations to warfare. But to sustain their power and confirm their worth as strategic and operational weapons requires modification of organizational structures supported by doctrine articulating the efficient and proper employment of technological innovations on each level of war. Past conflicts yield insights into how technology helps ensure victory. One aspect seems constant—formulating doctrine to exploit the full potential of technological innovation was a tedious process. Yet devising doctrine early is important to the expert use of information capabilities. An organizational structure grounded in doctrine guarantees the orderly development and effective employment of information age weapons.

On the strategic level the United States seeks to acquire, exploit, and protect information to support national objectives. Sectors for exploitation and protection include the economic, political, and military. Cultural as well as social information may also be required to support U.S. interests and strategic goals. On the operational level information warfare consists of attacking or defending information as well as exploiting it. Since information is critical to friend and foe alike, the object is the denial, deception, destruction, and attack of enemy information-critical systems.

Military doctrine codifies the belief about the best way to conduct military affairs. Doctrine is drawn most of all from experience. But past events may not be relevant in the information age. Current efforts to develop Air Force doctrine tend to treat information warfare as merely a new tool to enhance missions. It is not generally viewed as a weapon on its own merits. Since experience in information warfare is limited, doctrine for its use is



Global Hawk.

Teledyne Ryan Aeronautical (David Gossett)

Top Ten Information Warfare Targets

1. Culpeper (Virginia) electronic switch which handles all Federal funds and transactions
2. Alaska pipeline which carries 10 percent of all U.S. domestic oil
3. Electronic switching system which manages all telephony
4. Internet
5. Time distribution system
6. Panama Canal
7. Worldwide military command and control system (WMCSS)
8. Air Force satellite control network
9. Strait of Malacca, the major maritime link between Europe-Arabian Peninsula and the Western Pacific and East Asia
10. National Photographic Interpretation Center (Washington)

—Published in *Wired* magazine
(July/August 1993)

conflicting nations can no longer conduct political dialogue. It is the last resort if diplomats fail to produce an agreement. But are ideas promoted by Clausewitz still valid in the information age? He stressed the relationship between industrial age states in politics and war. An enemy in the 21st century may be as ambiguous as Clausewitz's depiction of the fog of war. When nation-states give way to transnational interest groups, who will the military fight? Over the next twenty to thirty

not easily derived. Developing information warfare doctrine results from an analysis of all the likely uses of information on all levels of war. In other words, an examination of how it is used as a national strategy mechanism is critical in addition to how it is employed on the lower levels of operational art and tactics. In all cases, both the offensive and defensive nature of information warfare requires detailed examination.

Clausewitz said that war "is a continuation of political intercourse, carried on with other means."

years the Armed Forces will confront diverse threats from advanced states to non-state actors such as terrorists. Knowing one's enemy is a timeless imperative in war. Therefore future doctrine must stress flexibility in strategy above all else. In Vietnam, strategic bombardment did little to change the course of the events. The lesson here is important: the love of technology must not deter the search for more effective and proper strategic alternatives.

Doctrine and strategy must account for the diverse mix of adversaries the Nation could face in the future. The threats range from a sophisticated enemy employing information technologies to the same extent as the United States to a rival totally devoid of high-tech capabilities.

A Sophisticated Enemy

The Persian Gulf War revealed the effectiveness and power of information age technologies and weaponry. Some regional powers are looking for ways to counter precision guided weapons, computers, and space-based assets. An information warfare attack on any information-advanced state may devastate its national infrastructure. Targeting financial, communications, electrical, and transportation nerve centers seriously impedes an enemy's ability to conduct war. Theoretically, victory is achieved without firing a single shot—at least a psychological victory demonstrating the will and resources of the attacker. Among advocates of information war this is the most discussed scenario. Sun Tzu instructs us, "to fight

and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.”

On the operational level information warfare seeks to distort and control the “adversary's perception of the battlespace by controlling or corrupting the information he uses, while providing the friendly commander with an unambiguous picture of his battlespace.”⁷ Techniques are used to defeat enemy information capabilities within battlespace constraints, including attacks on command and control network—the ability to maintain situational awareness and decisionmaking in the face of uncertainty—and the intelligence apparatus—the capacity to predict and anticipate the intentions and actions of friendly forces. Destroying these key elements at first opportunity is mandatory.

Space-based systems provide significant command, control, and intelligence capabilities to an enemy, perhaps equal to those of the United States. Thus a top priority of information warfare is enemy space systems. Taking out such assets quickly and precisely is paramount. Technology and weapons development in the near term must focus on neutralizing enemy eyes and ears in both air and space. Potential hardware and software weapons include anti-satellite munitions, precision bombs to strike ground stations, and software attacks against computers and networks. Tactically, this kind of warfare consists of electronic measures and physical destruction of information nodes.

Force Enhancement

Advanced systems can enhance our warfighting capability with superior command, control, communications, and intelligence networks. Their contribution during Desert Storm stimulated our appetite for high-tech systems. Current systems are routinely used in operations such as jamming radars, monitoring communications, and tracking movements. Future technology could enable us to impose electronic embargoes and detect vehicles or identify individuals on the battlefield.

Real-time or near real-time information on enemy locations, dispositions, capabilities, and indicators of intentions from surveillance and reconnaissance assets gives commanders situational awareness. Wide bandwidth digital communication systems afford real-time command and control links among commanders and units and between the National Command Authorities and globally-dispersed forces. Precision navigation systems, like the 24-satellite constellation that comprises the global positioning system, enhance weapons and delivery systems. Accurate weather

data enables direction of forces at the right time in support of tactical, operational, and strategic operations.

Information as Weapon

A successful information warfare offensive targeted at America would be a major disaster. Today an element of information dominance ensures that U.S. and allied systems are safe from any attack. The government, military, and industry must remain alert to attempts aimed at interrupting our activities. Enemy software penetration of the U.S. intelligence network or the communications infrastructure of a military commander could be fatal in war. Nations with emerging capabilities are known to target our systems. Terrorist groups and multinational organizations—to include the private business sector—also have keen interests in information sabotage.

The Internet attack in 1990 was perpetrated by an amateur. Professional computer hackers sponsored by hostile states or groups can do much more damage. And, as mentioned earlier, there are many computer specialists willing to offer their expertise to the highest bidder. Since the arena for hackers is the global network of computers and communications, information attackers may be as far away from their objectives as possible, unlike terrorists planting bombs. The covert nature of this endeavor is especially threatening.

Another trend hindering U.S. information dominance in war is the proliferation of military-relevant technologies outside the United States. According to one recent analysis,

*... precise navigation and imagery in the wrong hands can imperil U.S. forces. Space-based communications reduce the U.S. advantage in military command and control. Cryptologic capabilities could permit terrorists to plan havoc undetected.*⁸

Economically strong nations or groups freely purchase advanced technologies on the open market. Controlling the flow of such technology outside the United States or to radical actors is difficult. Most advanced systems have legitimate civilian applications. The military is increasingly turning to commercial products because of declining budgets. Dual use or sharing of commercial systems to support military operations, particularly communications satellites, may be the wave of the future. The fear lies in their vulnerability to attack and exploitation. Military systems are usually designed for security and survivability whereas civilian systems are not because of the costs involved.

information attackers may be far away from their objectives

Testing Dismounted Soldier System.



28th Public Affairs Detachment (William Cronk)

Cyber Warrior

integrated headgear—collects information for analysis and funnels latest intelligence to soldier in the field

lightweight helmet—provides greater protection with mounted display for night-vision sensors, miniature flat video panel, and voice activation for computer

body armor—allows room for computer while protecting soldier against nuclear and chemical hazards

thermal sight—sends multiple still-frames back to the high command, providing battlefield intelligence and damage assessment

computer—runs technology and gives soldier friend-or-foe identification, detects mines and chemicals, and tells exact location (embedded in lumbar region of body armor)

wireless connection—links weapon to monitor in helmet allowing soldier to take aim without exposing body

“All warfare is based on deception,” Sun Tzu once declared. “Hence when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.” Deception is a feature of warfare—in the 21st century deception will be information manipulation. Targeting information infrastructure to create misinformation, confusion, and panic is an objective. The results can be

disruption of society, economic collapse, elimination of decisionmaking ability, and reduced military effectiveness. Information warfare is useful in battle and a promising weapon of choice. Clausewitz’s dictum that war is simply an extension of politics by other means is also applicable to covert actions.

Far removed from physical harm, information warriors using the global network can attack information systems worldwide. Their strategic goals might include theft (stealing strategic plans), modification (inserting errors in databases), destruction (wiping out economic intelligence data),

and annihilation of infrastructure (introducing a software virus). With such tools the information warrior could change the course of an action by a potential enemy to favor U.S. policy.

The Gulf War demonstrated the decisiveness of information technologies. A new RMA is emerging with these capabilities at the center. An effective information warfare campaign depends on developing the doctrine and organizations to fully exploit its potential. At national level, covert information warfare against an enemy can help achieve policy objectives before committing forces. On the operational and tactical levels, it incapacitates enemy information-based systems, leaving its military confused while giving U.S. forces an overwhelming advantage in the field.

However potent such warfare is against a technologically advanced enemy, it must be used in a judicious and calculated way. Information warfare is not a panacea for all conflicts and cannot replace arms in combat. As in the past, knowing one’s enemy and how best to defeat it are crucial. History reveals the futility of employing advanced technology against an ill-defined enemy center of gravity. Recourse to information warfare must be objective and highly selective. **JFQ**

NOTES

¹ James R. FitzSimonds, “Intelligence and the Revolution in Military Affairs,” in *U.S. Intelligence at the Crossroads*, edited by Roy Godson et al. (Washington: Brassey’s, 1995), p. 375.

² Douglas Waller, “Onward Cyber Soldiers,” *Time*, vol. 146, no. 8 (August 21, 1995), p. 44.

³ Yoneji Masuda, “Computopia,” in *The Information Technology Revolution*, edited by Tom Forester (Cambridge: MIT Press, 1986), pp. 623.

⁴ Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), p. 7.

⁵ Judith Gunther, Suzanne Kantra, and Robert Langreth, “Digital Warrior,” *Popular Science* (September 1994), p. 63.

⁶ Edward D. Mansfield and Jack Snyder, “Democratization and War,” *Foreign Affairs*, vol. 74, no. 3 (May/June 1995), pp. 79–97.

⁷ U.S. Army Training and Doctrine Command, *Concepts for Information Operations*, pamphlet 525-6 (August 1995), p. 9.

⁸ Institute for National Strategic Studies, *Strategic Assessment 1995: U.S. Security Challenges in Transition* (Washington: National Defense University, 1995), p. 155.

This article is an edited and abridged version of an entry that received second prize in the 1996 JFQ “Essay Contest on the Revolution in Military Affairs” sponsored by the National Defense University Foundation.