1-1-1998

Information Operations and the Conduct of Land Warfare

Robert J. Bunker
Claremont Graduate University

INTERNET DOCUMENT INFORMATION FORM

A. Report Title: Information Operation and the Conduct of Land Warfare

B. DATE Report downloaded From the Internet: October 12, 2000

Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): AUSA's Institute of Land Warfare, 2425 Wilson Bldg. Arlington, VA.

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: __LL__ **Preparation Date October 19, 2000**

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.

Information Operations and the Conduct of Land Warfare

by

Robert J. Bunker

The Institute of Land Warfare
ASSOCIATION OF THE UNITED STATES ARMY

AN AUSA INSTITUTE OF LAND WARFARE PAPER

The purpose of the Institute of Land Warfare is to extend the educational work of AUSA by sponsoring scholarly publications, to include books, monographs and essays on key defense issues, as well as workshops and symposia. A work selected for publication as a Land Warfare Paper represents research by the author which, in the opinion of the editorial board, will contribute to a better understanding of a particular defense or national security issue. Publication as an Institute of Land Warfare Paper does not indicate that the Association of the United States Army agrees with everything in the paper, but does suggest that the Association believes the paper will stimulate the thinking of AUSA members and others concerned about important defense issues.

LAND WARFARE PAPER NO. 31, OCTOBER 1998

Information Operations and the Conduct of Land Warfare

by Robert J. Bunker

Dr. Robert J. Bunker is an adjunct professor in the National Security Studies program at California State University, San Bernardino and a professor, unconventional warfare, with American Military University. He holds a Ph.D. in Political Science from the Claremont Graduate University. His research focus is on the influence of technology on warfare and political organization and on the national security implications of emerging forms of warfare. Dr. Bunker has published numerous articles and reports and has served as a consultant to both military and law enforcement agencies. He was a speaker at the Ninth Annual Strategy Conference, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 31 March-2 April 1998.

Inquiries regarding this and future Land Warfare Papers should be directed to: Association of the United States Army, Institute of Land Warfare, telephone: 1-800-336-4570 or 703-841-4300, extension 631.

Contents

Foreword

Information operations will represent a core Army XXI capability. They will allow for unprecedented battlespace awareness, increased speed and tempo in land warfare and, ultimately, for Army information dominance. These expectations must be tempered with the knowledge that they represent the institutional Army view of information operations. Other views exist which challenge current Army warfighting assumptions.

The central argument developed in this important paper concerns whether information operations will be an adjunct to current operational methods, basically a force multiplier, or a totally new operational mechanism which will provide warfighting capabilities which heretofore did not exist. Both schools of thought are analyzed in this paper along with a discussion of information operations definitions and target sets and the land warfare implications of information operations.

The value of this paper is derived from its ability to generate debate on an issue of central importance to the Army. As the victors of the Cold and Gulf Wars, our approach to information operations is inherently more conservative than that of many of our future opponents, some of whom will rely upon cyberterrorism and other asymmetric attempts to overcome our battlefield advantages. Thus, while information operations will allow us to greatly advance our traditional warfighting capabilities, we must recognize that they may open up new warfighting venues which will need to be explored and debated to ensure that the Army retains its battlefield dominance into the early 21st century.

GORDON R. SULLIVAN
General, U.S. Army Retired
President

October 1998

Information Operations and the Conduct of Land Warfare

This paper focuses on the implications of information operations (IO) on the U.S. Army's conduct of land warfare over the next decade.[1] This transitional period from the experimental Force XXI to the digitized Army XXI offers many promises, potentials and even pitfalls for the world's predominant land power force. BG James M. Dubik, USA, has recognized this in his earlier Institute of Land Warfare paper *Creating Combat Power for the 21st Century*.[2]

The term "information operations" conjures up many images. To some the vision of Heinlein's classic *Starship Troopers* comes to mind with its Mobile Infantry (M.I.) forces in high-tech body armor.[3] Armed with vast amounts of individual firepower and linked into information nets, these soldiers provide one archetype of the future Army force. Another vision is at odds with the high-tech warrior tradition. It is that of out-of-shape armchair soldiers sitting behind their computer terminals launching war-winning cyberattacks at the stroke of a key. A third vision is derived from the cyberpunk genre. It is that of Johnny Mnemonic-type individuals, with hardwires in their brains and enough downloaded information to make a modern supercomputer look like a kid's cheap toy.[4] Such enhanced individuals would give a whole new meaning to the concept of the "special forces" of the future and, while some truth probably exists in each of these visions, for now that is all they are — visions of the future.

No underlying thesis or policy will be consciously promoted in this paper with regard to the Army's relationship to information operations except for the self-evident fact that they are becoming increasingly critical to its continued battlefield dominance. The paper has two goals: First, by focusing on the important transitional period we are now facing, this paper will show the basis of information operations thinking and the two competing schools of thought which have developed, outlining areas of potential synthesis between them. Second, this paper will assess the potential impact of these operations on land warfare and analyze some of the issues associated with them.

At the outset, however, current definitions and perceptions of information operations, and ultimately of information itself, will be reviewed and discussed in hopes of seeing the divergence in and perhaps coming closer to a common frame of reference to guide the following discussion.

Defining Information Operations

"Information operations" is a relatively recent term. In the current Army Field Manual (FM) 100-5, *Operations*, June 1993, the term is not even mentioned.[5] Early definitions of this term can be found in U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-5, *Force XXI Operations*, 1 August 1994:

> Continuous combined arms operations that enable, enhance, and protect the commander's decision cycle and execution while influencing an opponent's; operations are accomplished through effective intelligence, command and control, and command and control warfare operations, supported by all available friendly information systems; battle command information operations are conducted across the full range of military operations.[6]

and in FM 100-6, *Information Operations*, of 27 August 1996:

> Continuous military operations within the MIE [Military Information Environment] that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE [Global Information Environment] and exploiting or denying an adversary's information and decision capabilities.[7]

The value of information to the conduct of land warfare has been commented on by General Dennis Reimer, Army Chief of Staff. On 4 September 1996, he stated, "The evolving military information environment will fundamentally change the way we, the Army, conduct operations in peace and conflict. IO includes all measures, both offensive and defensive, taken to achieve information dominance. The Army will integrate IO into every aspect of Army XXI."[8]

Two years later, some debate exists concerning the nature and value of information operations to Army XXI. Early Army definitions are in variance with current Joint Force perceptions. Further, while information operations are recognized as being potentially of great value, their actual value to date is disputed. One school of thought posits that they represent an adjunct to current operations — the end result of which is to enhance current Army capabilities by making what it has traditionally done better by means of a force multiplier effect. Another school of thought suggests that information operations will provide the Army with new capabilities. Instead of being a simple adjunct to current operations, according to this school, the influence of the "information revolution" on warfare will result in the redefinition of operations themselves. Both schools do agree that information operations has become a dominant, albeit at times ambiguous, concept for Army professionals to wrestle with.

As can be seen even within the Army, one of the maddening aspects of information operations is defining them. This is particularly troublesome for those who did not grow up with computers and who inherently do not feel comfortable working with them. Further, information operations has become something of the current buzz word. Pepper your conversation a few times with the term and it shows you are up to date concerning cutting edge military thinking. Another major problem with the term is that two individuals can be discussing it and talk right past each other. An Internet-based attack, the use of propaganda, and even terrorism can be labeled as forms of information operations. Unless the individuals can agree upon the broader definition of the term, their examples have little in common with each other. Let us now look at the Joint Force definition of information operations and a number of typologies of the concepts involved.

The best information operations (IO) definition is currently provided by the Department of Defense. They are defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[9] While, as viewed previously, early Army definitions were subordinated to more traditional commander and force needs, the Joint Force definition is much more abstract in nature.[10] It literally decouples the concept of operations from the physical environment in which the Army is used to campaigning. As an outcome, cyberspace takes on its own form of existence and becomes, in its own right, a form of battlespace where information operations can be conducted. For those soldiers who think solely in terms of tanks, helicopters and artillery pieces, this conceptual leap is extremely difficult to grasp, much less accept.

Information warfare (IW), in turn, is conceptually subordinated to information operations. It is defined as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[11] The basic concept behind Joint Force information operations can be expressed in table form for better ease of understanding (see table 1).

Table 1. Basic Information Operations

Defend Our	Attack Their
Information	Information
Information Systems	Information Systems

The question which must then be asked is, "What is meant by information and information systems?" The definition of information used in *Concept for Future Joint Operations: Expanding Joint Vision 2010* is "data collected from the environment and processed into a usable form." [12] Data is in turn defined as "representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means. Any representations such as characters or analog quantities to which meaning is or might be assigned."[13] Based upon these perceptions, an information attack upon an opposing force results in the disruption of its cognitive hierarchy. This is done by targeting data — a processing function. This will directly affect higher-level functions such as cognition and judgment.[14]

An earlier information typology was provided in *War in the Information Age*. It divides information as follows:

> Four basic forms of information will form the core upon which America's information age Army procedures and organizations will be built. First is *content information*, the simple inventory of information about the quantity, location and types of items. Second is *form information*, the descriptions of the shape and composition of objects. Third is *behavior information*, three dimensional simulation that will predict behavior of at least physical objects, ultimately being able to "wargame" courses of action. Finally, *action information* is the kind of information that allows operations to take the appropriate action quickly.[15]

The attack and defense of each of these four forms of information could also fit into the information operations mandate. In the more recent *Athena's Camp*, three views of information are discussed: "The first considers information in terms of the inherent *message*, the second in terms of the *medium* of production, storage, transmission, and reception. The emerging third view transcends the former two; it speculates that information may be a *physical property* — as physical as mass and energy, and inherent in all matter." [16] The first view generally compliments the *Joint Vision 2010* processing definition based upon information operations directed against data. It also seems to include information which is viewed as "organized data" — as opposed to raw data, which is disjointed in nature because it has not been processed through some sort of filtering system. The second view, which is medium- or conduit-based, would appear to fall under the rubric of information systems rather than information. It will be discussed later.

The third view based upon information as a physical property, a structuralist perspective, proposes:

> Information is as basic to physical reality as matter and energy — all material objects are said to embody not only matter and energy, but also "information." The spectrum for this view runs from modestly regarding information as an output of matter and energy; to regarding information as equal in importance to matter and energy; to regarding information as even more fundamental than matter and energy. Information, then, is an embedded *physical* property of all objects that exhibit organization and structure. This applies to dirt clods as well as DNA strands.[17]

While this cutting edge scientific view will have many implications for future information operations, in tandem with the development of the new sciences of chaos and complexity theory and other postmechanical and nonlinear disciplines, it will more heavily influence the Army After Next (AAN) than the more immediate Army XXI. [18]

Over the course of the next decade, it is probably more useful to view two forms of information existing based upon message and processing considerations. The first form, *data*, is raw, disorganized and unfilitered in nature. The vast majority of battlespace information is gathered from human and electronic sensors. The second form, *information*, represents data which has been filtered and organized by human and electronic processors. Information represents a smaller, but more valuable, resource pool than data and is only as good as the validity of the data provided and the sophistication of the processor involved.[19] Many information-specific typologies can exist, including the previously mentioned one based upon content, form, behavior and action information.

The question concerning what is an information system must now be addressed. In *Concept for Future Joint Operations* this is defined as:

> Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations, by collecting, processing, analyzing, archiving, and disseminating information.[20]

The current Special Forces definition represents a variation on this theme: "The personnel and equipment to manage, display, transport and disseminate information needed for rapid decision making necessary for victory."[21] The medium view mentioned earlier suggests that such a system is composed of information production, storage, transmission and reception.

Probably the most useful way of defining a generic information system is to recognize that it requires seven basic components to minimally function.[22] These are *sensors* which provide data, *processors* who filter and organize it into information, *receptors* who utilize it, *databases* where data and information is stored, *transmitters* who disseminate data and information, *rules* which define system operation and structure, and *synergy* which allows a system to function better than the total sum of its parts. These components are not mutually exclusive. A receptor, for example, might be a decisionmaker or a trigger-puller or could just as well be a sensor which has been provided with new information concerning its sensing mission. What must also be recognized is that an individual soldier or a tank and its crew can be thought of as a miniature information system form even though the system which is being discussed in this paper applies to Army XXI itself. An applied view of information operations can now be expressed (see table 2). It provides the conceptual basis from which the conduct of Army XXI information operations can be discussed.

Table 2. Applied Information Operations

Defend Our	Attack Their
Information • Data • Information	Information • Data • Information
Information Systems • Sensors • Processors • Receptors • Databases • Transmitters • Rules • Synergy	Information Systems • Sensors • Processors • Receptors • Databases • Transmitters • Rules • Synergy

Army XXI Information Operations

Derived from table 2, nine basic target sets exist in information operations. These target sets can be applied against the popularized notion of the Clausewitzian trinity of a nation-state represented by its military, government and people. Army XXI information operations, by necessity, will focus upon the military informational environment. However, attributes of the informational environments belonging to the government and the people will impact the success of Army XXI on the battlefield. Increasing Army reliance upon civilian Internet switches represents one example. If the Internet were to become disrupted by hackers, operating independently or in the employ of a foreign government or criminal

organization while a military operation was in progress, information exchange between Army units could become severely disrupted. Another example can be derived from a recent incident. On 25 June 1998, the computerized reservation system belonging to American Airlines went down for three hours for unknown reasons. Flight delays resulted which ranged from 15 minutes to two hours.[23] Civilian carriers provide the Army with an additional surge capability to project its forces immediately. If the reservation systems of these carriers were targeted on an ongoing basis, the resulting chaos could disrupt such a surge capability, not to mention the massive problems it would generate for business professionals and other air travellers.[24]

When specifically applied to the military information environment, these nine target sets can be broken down into two derived from information and seven derived from characteristics of information systems. Data which have been obtained by sensors and information generated by processors can be attacked in three basic ways: by means of destruction, degradation and alteration. The destruction of data and information is very straightforward. A string of 0s and 1s representing bits of information is eliminated. Degradation of data and information is the partial elimination of a string of 0s and 1s so that message gaps appear. Data and information alteration is the resequencing of a string of 0s and 1s.[25]

Of these three forms of attack, alteration is the most threatening but also the most complicated to undertake. It can not only result in wrong decisions and actions being made but also pollutes the data and information belonging to a military force. This can produce ambiguity within a force concerning the validity and reliability of sections of its knowledge pool. For example, if the text of an online helicopter repair manual, say for the AH-64D Longbow Apache, were altered leading to a disaster for either the helicopter crewmen or the ground crew, all online repair manuals would become suspect. Unless proofed line-by-line or, far more likely, reloaded from secure backups protected by strong firewalls or physical air-gaps, their use would be denied to Army personnel. Digital destruction, on the other hand, would result in the erasure of data and information which would be quite obvious, would not result in faulty helicopter repairs being made, and is more easily solved. Possibly a more insidious example would be that of changing the dosage of medications for Army personnel or altering the information concerning the effects of prescribing two medications together so that fatal or near-fatal combinations could result.

Sensors, which range from close-in to stand-off forms, can be targeted by denying them data, altering the data provided, disrupting their sensing capabilities or destroying their capability to function. Data denial would focus on electromagnetic signature suppression and other techniques such as frequency-hopping broadcasts so that sensors are unable to gather data. Data alteration allows sensors to obtain data that the opposing force wants to be obtained. This could allow a tank to broadcast a truck signature and vice versa or create the illusion that more forces exist than really do. Disruption of sensing capabilities can be undertaken by providing "noise" in the appropriate segment of the electromagnetic spectrum to achieve a masking effect or by the employment of obscurants which can be used to coat the surfaces of sensing devices, making them opaque to electromagnetic radiation. Sensor destruction can be achieved physically, by targeting them with

conventional weaponry or by nonlethals such as destructive microbes, or nonphysically via electromagnetic pulse which would burn out their components.

Processors, both human and machine, can be attacked in order to degrade or influence analysis and decisionmaking functions. Providing processors altered data, via the sensors of their information net, would be the most basic form of such an attack because skewed data input results in skewed information output. Machine processors can also be targeted by corrupting their algorithms with a virus or providing them, as in the case of expert systems, with contradictory instructions which can result in the machine equivalent of a nervous breakdown. Humans, on the other hand, suffer greatly when faced with excessive ambiguity. If a human decisionmaker, such as a foreign military commander, can be purposefully targeted in this regard, his or her analytical process will suffer. Further, humans have a number of basic biological needs, such as sleep, and if such needs can be denied to them for extended periods of time their decisionmaking capabilities will become severely degraded.

Receptors are vulnerable to sender deception. They can be made to either believe that information being sent to them is false, as in the case of its appearing to come from an opposing force when it is coming from their own force, or that information which is being sent to them is true, as in the case of its appearing to come from their own force when it is coming from the opposing force (i.e., spoofing). In the first instance, information is not being accepted when it should be, and in the second instance, information is being accepted when it shouldn't. Both forms of sender deception can cause confusion and disruption to an opposing force. Anything from e-mail messages to phone conversations to digital radio transmissions to videotapes can be affected in this manner.

Databases represent the physical hosts and mediums in which data and information are stored. This hardware, like all hardware, is susceptible to physical and upper-tier nonlethal attack. While less sophisticated than targeting data and information itself via cyberspace, database targeting will result in either informational destruction or the denial of its use until database repairs are made or the surviving information they contain is salvaged and transferred to another database.

Transmitters are representative of communication devices and protocols. These are susceptible to traditional forms of attack based upon electronic warfare, jamming measures, and precision fires. As in conventional operations, this is one of the most desirable target sets to attack because it provides the informational linkages within and between military units.

Rules such as standard operating procedures, the laws of war, and military ethics moderate and regulate warfare.[26] Rules help to establish warfare as a legitimate form of organized political violence (i.e., an extension of politics by other means) between sovereign states as opposed to mass murder, ethnic cleansing, terrorism and other forms of criminal activity waged by nonstate actors and illegitimate despots. Western rules of war are easy to attack because they represent artificial political conventions. By removing their uniforms and military insignia from their vehicles and mixing themselves in with civilian

populations, many non-Western forces actively engage in applied information operations against U.S. forces.

Synergy in an information system results in a military force gaining battlefield advantage by fusing together the individual contributions of its components into something greater than the sum of its parts. This synergy allows for faster OODA (Observe-Orient-Decide-Act) loops, reaction times and decision cycles to take place. By understanding an opposing force's information system process this synergy can be attacked and degraded, disrupted or destroyed as an outcome of coordinated attacks upon the other information operations target sets. As an example, the complete disruption of any one category of target sets, such as transmitters, will cripple an information system. Attacking the proper combinations of target sets may also achieve this desired effect by means of a cascading effect.

Based on the above typology, Army branches can attack specialized parts of an adversary's information and information system, and also help to protect their own assets. The tasking model used by U.S. Army Intelligence and Security Command (INSCOM) breaks down information operations into those units/functions which defend information, attack information and provide information operations enablers (see table 3).[27] Such actions can be active or passive in nature. A secure firewall between brigade networks would represent a passive form of defense, while installing Blitzkrieg software, which recognizes hacking attempts and repels them, would be an active form of defense.[28] The INSCOM model appears to be but one approach to undertaking information operations. Because this concept is so new and dynamic, no general Army consensus exists in regards to which combat, support or service branch should undertake which information operations mission.

Table 3. INSCOM Information Operations Model[29]

Defend Information	Attack Information	Information Operations Enablers
• Operations Security • Information Security • Communications Security • Computer Security • Physical Security • Network Management • Counter Deception • Counter Psychological Operations • Counterintelligence • Law Enforcement Liaison	• Electronic Warfare • Computer Network Attack • Psychological Operations • Special Information Operations • Physical Attack • Deception	• Public Affairs • Civil Affairs • Intelligence • Support • Battle Management Command, Control & Communications

Competing Views of Information Operations

As discussed in the introduction to this paper, two schools of thought exist in regard to the significance of information operations. The major perceptions of these schools of thought are highlighted below:

The Force Multiplier School. The operational concepts developed in *Joint Vision 2010* — dominant maneuver, precision engagement, full-dimensional protection, and focused logistics — are derived from informational superiority and other joint warfighting capability objectives. Information superiority, however, is the only objective which is integral to all four operational concepts.[30] Such superiority is defined as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[31] This form of strategic guidance allows Army XXI to become better at what it already does, which is to seize terrain and destroy opposing conventional military forces belonging to other nation-states. Such traditionalist concepts fully complement initiatives to take the current mechanized force of Bradley Fighting Vehicles, Abrams Tanks, et al. and digitize them via appliqués.

Wired fighting vehicles, artillery and helicopters benefit from information operations by means of sensors which can better identify opposing forces, thus minimizing the "fog of war" and providing what is termed dominant battlespace knowledge.

> An interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it.[32]

The logic goes that if an enemy can be sensed, he can then be fixed in time and space, and killed with precision munitions or neutralized with nonlethal force. Such advantages as this will allow Army units to project current combat power levels with fewer personnel. As a case in point, Army heavy division size is currently being reduced from more than 18,000 to 15,700 soldiers because of efficiencies caused by information technologies in logistics.[33] It should be noted that this personnel savings comes prior to a division digitization, slated to take place in 2000, and a corps digitization scheduled for 2004.[34]

Virtually all aspects of Army operations can be made more efficient via information technologies. In the case of nonstate war in urban environments, lessons learned from the recent Russian debacle portray the utility of these operations:

> One of the major insights gained from the Russian experience in Grozny concerns information dominance. The importance of being able to control broadcasting capabilities, suppress inflammatory information, influence attitudes, and hamper or intercept information flow within hostile elements was abundantly clear. Russian forces were unable to do these things and suffered accordingly. Given the array of communications links — TV, radio, telephone, cellular phone, internet, etc., the challenge of achieving information dominance is formidable.[35]

Fortunately, in Bosnia, such mistakes were avoided by Army and allied forces in Operation Joint Endeavor. In fact, a well-coordinated information campaign based on publication information (PI), psychological operations (PSYOPS), and civil-military cooperation (CIMIC) was undertaken.[36]

Even with these many benefits, challenges exist in regard to information operations as a whole. One concerns how to get information to tactical units and back to the commanders. The older communications structure was built upon voice and low speed data transmissions while "the information component of future military operations will primarily be comprised of computer data, imagery, video and much less voice commo than in the past."[37] Another challenge may exist in regard to the potential for micromanagement by senior officers and junior officers becoming overloaded with too much information. Issues such as this will need to be explored and solved if problems do arise. As an outcome of digitization, hierarchical thinking will be replaced with a more networked approach to warfighting. This will offer new opportunities in regard to fighting toward a common battlefield image but will also result in potential dilemmas in regard to the current organizational structure, with some formations and possibly even rank structures no longer potentially needed as Army units get flatter.

What is known is that commercial technology will begin to provide an increasing segment of the hardware Army XXI will rely upon. This exploitation of commercial technology will provide the Army with many advantages in regard to technical breakthroughs but must be tempered with the realization that such technology can be bought on the global market by anyone.[38] While the force multiplication effects of information operations are fully recognized, the cost of digitization is becoming an increasing concern. The Commandant of the Marine Corps has stated that his service cannot afford digitization and suggests that to a degree this may also be true for the Army because of the declining defense budget.[39] If this is the case, then Army XXI may ultimately comprise only selected divisions of the Army who will gain the full benefits that information operations will provide.[40]

The New Capabilities School. It has become an accepted fact that nonstate challengers and rogue nation-states have no hope of taking on and defeating the premier landpower force in the world today in conventional warfare. The Army is simply too good at what it does. The down side of ruling the battlefield is that our opponents have no choice but to replace symmetrical warfighting with asymmetrical counters when facing the Army. On a physical level, they are exploring new combat capabilities based upon weapons of mass destruction. Nuclear, biological and chemical weapons offer many possibilities especially when used by small terrorist cells which cannot be traced back to their employers.

Our focus, however, is in regard to the digital or cyber dimension. Information operations allow criminal, guerrilla and other rogue entities a new operational style which previously did not exist. A force multiplication effect is useless to such entities because they have no traditional combat power to multiply. Rather, information operations in this regard are more visionary in nature and represent an asymmetric form of warfare based upon what could be termed "weapons of mass disruption."[41] This potential has not gone

unnoticed by governmental authorities with regard to the threat posed to our nation's infrastructure.[42] One National Defense University researcher has observed:

> The implications of warfare in the information arena are enormous. First, national homelands are not sanctuaries. They can be attacked directly, and potentially anonymously, by foreign powers, criminal organizations, or nonnational actors such as ethnic groups, renegade corporations, or zealots of almost any persuasion. Traditional military weapons cannot be interposed between the information warfare threat and society.
>
> Second, even where traditional combat conditions exist (hostile military forces face one another in a terrain-defined battlespace), kinetic weapons are only part of the arsenal available to adversaries. Indeed, electronic espionage and sabotage, psychological warfare attacks delivered via mass media, digital deception, and hacker attacks on the adversaries' command and control systems will be used to neutralize most traditional forces and allow concentration of fire and decisive force at the crucial time and place in the battlespace. [43]

Examples of this new operational style mentioned in another National Defense University paper include:

- A "trap door" hidden in the code controlling switching centers of the Public Switched Network could cause portions of it to fail on command.
- A mass dialing attack by personal computers might overwhelm a local phone system.
- A "logic bomb" or other intrusion into rail computer systems might cause trains to be misrouted and, perhaps, crash.
- A computer intruder might remotely alter the formulas of medication at pharmaceutical manufacturers, or personal medical information, such as blood type, in medical databases.
- A concentrated e-mail attack might overwhelm or paralyze a significant network.
- An "infoblockade" could permit little or no electronic information to enter or leave a nation's borders. [44]

For information concerning similar concepts, refer to Appendix 1, Army War College IW Tutorial Terms. Conceptually, this form of warfighting can be considered a form of bond-relationship targeting (i.e., the links between things) as opposed to precision strike, which targets things themselves. A proposed definition for this form of operations is as follows:

> Rather than gross physical destruction or injury, the desired end state is to create tailored disruption within a thing, between it and other things, or between it and its environment by degrading or severing the bonds and relationships which define its existence. [45]

Because Army special operations forces do not rely upon forms of traditional combat power as do conventional Army forces, it would seem that they would be more apt to view information operations as a new capability rather than as a force multiplier like nonstate groups. If this is the case, they may begin to rely upon offensive information operations as a primary means of disruption attack against opposing forces. Within the next decade, lessons learned by Army special operations forces may offer little utility to conventional forces in this regard; however, in the long run, what is now considered an unconventional form of information warfare could become the new norm.

In addition to Army special operations forces, the employment of IO by private security corporations is another trend which must be considered. The Army's recent decision to choose Internet Security Systems, Inc., to defend its cyber-assets in over 400 U.S. Army facilities worldwide suggests that the private sector may be more adept than traditional military institutions at waging war within higher-dimensional battlespace. [46] If this is the case it would represent an ominous trend because cyberspace would ultimately help to undermine the warmaking monopoly held by the public institutions of the nation-state, as it is already doing to concepts of national sovereignty.

Land Warfare Implications

Of the two schools of thought previously discussed, the perception of information operations as a force multiplier will presumably dominate over the course of the next decade or so within Army circles — out to about 2010. Army XXI by necessity will exist in two worlds — partially mechanical and partially digital. First, it will draw its firepower largely from preexisting hardware that was designed for the Cold War security environment.[47] The hardware sunk costs and preexisting training and support base dictate no less in an era of declining defense expenditures.

At the same time, most of the Army's senior leadership will still be traditionalist in its view of the influence of technology, especially information technology, on the conduct of land warfare. Bolted onto this hardware will be information devices which will multiply its combat power and effectiveness. Given such a near-term scenario, information operations will be viewed as a means to an operational end, that is, as a force multiplier for conventional operations and probably not as a viable operational style in itself.

The primary danger which exists with traditionalist-school thinking is that of being lulled into a false sense of security. Because Army XXI will be so far in advance of its nearest competitors, it may become fashionable to suggest that no one will ever be able to catch up to the Army in warfighting capacity. This would assume that information operations will remain subordinate to conventional operations over the long term. As a result, land warfare forces would retain their current capabilities and continually refine them.[48] No basis exists to support such an assumption. Rather, it is suggested that information operations may mature to the point of becoming an operational style in itself and/or fuse with conventional operations to become a dual-dimensional operational hybrid which is physically- and cyber-based. This maturation will develop primarily because of the development of asymmetric attempts of our opponents at undermining Army XXI combat

power, Army special operations forces experimentation in these areas, growing private security information operations capability, and the recognition of these trends by senior Army leaders.[49] This would result in the development of a whole new battlefield upon which the Army After Next, rather than Army XXI, will be more suited to function.[50]

This perception brings up two land warfare issues which need to be further studied with regard to information operations. The first concerns the impact of advanced technology and concepts on land warfare. Do such technologies and concepts tend to get designated as force multipliers by the dominant army of the era (the winners) to allow it to do what it does even better? This would be in contrast to such technologies and concepts being designated as a new form of operations by inferior armies or groups (the losers) who have no stake in the prevailing military status quo. A historical example of this phenomenon is represented by the development of the tank in the 1920s and 1930s. For the allies in World War II, the tank was early on considered an infantry support weapon which provided mobile firepower, hence a force multiplier, rather than a key element of a new operational concept as was then developed by the German army. Another example of this phenomenon would be the development and employment of functional field artillery, coupled with the levee en masse and other innovations by the French during its Revolutionary Wars of the late 18th and early 19th centuries. This "loser" army of the late Absolutist age went on to redefine warfare between the armies of nation-states because it saw the advanced technology and concepts which had developed as the basis of new operations and not as a force multiplier as did its competitors.

The issue of advanced technology and concepts either as a force multiplier or as the basis of new operations will heavily impact the future Army. It will likely result in the development of a second issue — when, and if, the Army should organize itself around qualitatively new operational styles. As previously mentioned, out to 2010 or so information operations as a force multiplier will presumably dominant conventional Army force thinking, and rightly so. From 2010 on, however, information operations as a real operational style in itself and/or as part of the basis of a dual-dimensional operational hybrid will begin to make itself more pronounced. The time frame from 2010 to 2025 may thus become a critical period for Army planners. It will represent the last vestiges of Cold War-influenced combat hardware mated to digital appliqués and the introduction of qualitatively new systems which possess organic informational abilities and the new operational capabilities they will provide.[51]

In the short term, however, the future looks bright with regard to the transition from Force XXI to Army XXI and continued Army land warfare dominance with the addition of information operations as a force multiplier. The Army is second to none as a landpower force and can no longer be defeated in a traditional battlefield setting with conventional arms and tactics. This recognized invulnerability, however, is both a blessing and a bane because, as discussed in this paper, America's opponents will ultimately attempt to turn information operations into the Army's Achilles' heal.

Appendix 1

Army War College IW Tutorial Terms[52]

Cryptology: Cryptology is a weapon of information warfare designed to encrypt and crack secure communications respectively. Despite significant advances in cryptography, cryptanalysis will continue to be an important weapon aided by equally significant advances in computing power.

Decision Support: As in any decision process, the more information available the higher the probability of arriving at a useful solution. Likewise, computer decision support is also a key weapon in information warfare and especially in defensive information warfare. Decision support can be used to detect attacks, identify the type of attack, generate defensive options, evaluate options, and perform damage assessments. In a similar manner, an adversary's decision support system can be delayed, or disrupted with erroneous data.

Destructive Microbes: Researchers are also working on developing microbes which eat electronics components so that, in the event of conflict, these microbes could be introduced into an adversary's electronics equipment to cause failure.

Electromagnetic Pulse: Electromagnetic pulse weapons could be used to knock out enemy electronics equipment. Suitcase-sized devices have been developed to do just that.

Infrastructure Attacks: Various possible operations with obvious effects include knocking out telephone switches, crashing stock markets, attacking electronic routers for rail systems, attacking bank accounts, disrupting air traffic control, and denying service with, for instance, a ping attack. Note: The "ping" attack gets its name from old age sonar techniques. Within a network, a computer can send systematic queries to all addresses and analyze the associated return time, very similar to sonar. Net groups with similar times of return can be associated into a hierarchical structure.

Malicious Software: Viruses: computer programs that can infect systems and cause damage. They are usually hidden within safe-looking programs (usually shareware or freeware). Trojan horse: a computer program that enables the disseminator of the program to access the system that interacts with the program. A Trojan horse is different from a virus in that a virus can be duplicated thousands of times and function according to a previous set of instructions, while a Trojan horse is designed to facilitate access and interaction between its creator and the system it infiltrates. Worm: a computer program that infests network environments and copies itself over and over again. Worms can take up more and more memory and disk space until they stop the computer cold. The famous Internet worm of November 1988 replicated itself on more than 6,000 networks around the world. Clipper: hardware that can automatically encrypt and decrypt data. It has a trapdoor which would enable federal authorities to open with a key and monitor data.

Psychological Operations: Psychological operations (PSYOPS) using all available information means to form a desired public opinion. PSYOPS benefits from the ability to conduct market research and analysis of regional data. As a result, customized messages

can be generated for each target sector of society. PSYOPS was very successful in the U.S. reinstatement of Haiti's president.

Spoofing: Spoofing is an attempt to send a falsified message to someone. For example, I could dial up a university phone registration system pretending to be someone I have a grudge against, and drop their classes. Since these systems are automated, all I would need to know in most cases is a person's Social Security number and birthdate.

Stand-Off and Close-In Sensors: For military applications, the use of stand-off and close-in sensors to gather data could be considered an information warfare weapon.

Van Eck Radiation: Van Eck radiation is the radiation which all electronic devices emit. Specialized receivers can pick up this radiation and tap a wealth of information. Fortunately, there are various safeguards against this type of attack.

Video Morphing: Video morphing is a weapon that could be used in a manner similar to that in the movie "Forrest Gump" to make an enemy leader appear to say things he or she didn't in fact say, undermining credibility.

ENDNOTES

1. For a complete listing of documents related to information operations on compact disc, see Land Information Warfare Activity at http://www.sytexinc.com/cdrom/background/pubs.htm; for an excellent set of annotated information warfare references complied by Daniel E. Magsig, go to http://carlisle-www.army.mil/usacsl/org/iw/tutorial/intro.htm and click on "References."

2. James M. Dubik, *Creating Combat Power for the 21st Century*, Land Warfare Paper No. 25 (Arlington, Va.: The Institute of Land Warfare, Association of the United States Army, October 1996).

3. Robert A. Heinlein, *Starship Troopers* (New York: G.P. Putnam's Sons, 1959).

4. William Gibson, *Johnny Mnemonic* (New York: Ace Books, 1995).

5. Headquarters Department of the Army. FM 100-5, *Operations* (Washington, D.C.: U.S. Government Printing Office, 14 June 1993).

6. TRADOC Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century* (Fort Monroe, Va.: U.S. Army Training and Doctrine Command, 1 August 1994), p. Glossary-4.

7. Headquarters Department of the Army. FM 100-6, *Information Operations* (Washington, D.C.: U.S. Government Printing Office, 27 August 1996). Access via http://www.atcs-army.org/cgi-bin/atdl.dll/query/download/fm/100-6/fm100-6.zip.

8. Cited in MG John D. Thomas, Jr., Commanding General, U.S. Army Intelligence and Security Command, "Impact of Information Operations for the Force XXI Army" (Fort Belvoir, Va.: U.S. Army Intelligence and Security Command), briefing slides presented at the Association of the United States Army Symposium and Exhibition, "The Role of Special Operations Forces in Information Operations" Pinehurst, N.C., April 7, 1998.

9. U.S. Department of Defense. Department of Defense Directive – Supplement (DODD-S) 3600.1, *Information Operations*, 9 Dec 96.

10. Later Army perceptions fall within the *Joint Vision 2010* conceptual umbrella. See *Army Vision 2010* at http:www.army.mil/2010/.

11. DODD-S 3600.1.

12. Joint Chiefs of Staff, *Concept for Future Joint Operations: Expanding Joint Vision 2010* (Fort Monroe, Va.: Joint Warfighting Center. May 1997), p. 85. Derived from Joint Pub 6-0.

13. Ibid., p. 83. Approved DoD terminology.

14. Ibid., p. 85.

15. GEN Gordon R. Sullivan and COL James M. Dubik, *War in the Information Age* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, June 6, 1994), p. 18. Derived from William H. Davidow and Michael S. Malone, *The Virtual Corporation* (New York: Harper Collins Publisher, 1992), pp. 67-72.

16. John Arquilla and David Ronfeldt, Chapter Six, "Information, Power, and Grand Strategy: In Athena's Camp – Section 1," John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: National Defense Research Institute, RAND, 1997), pp. 144-145.

17. Ibid., p. 148.

18. For an overview of the challenges these sciences and disciplines may pose for the Army After Next see Robert J. Bunker, *Five-Dimensional (Cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, March 10, 1998).

19. This typology draws from Figure 19.1 – "The 'Information Pyramid' from Two Views," John Arquilla and David Ronfeldt, Chapter Nineteen, "Looking Ahead: Preparing for Information-Age Conflict," *In Athena's Camp* p. 448.

20. Joint Chiefs of Staff, *Concept for Future Joint Operations*, p. 86.

21. BG John R. Scales, Deputy Commanding General, U.S. Army special Forces Command (Airborne), "Information Operations" (Fort Bragg, N.C.: U.S. Army Special Forces Command (Airborne)), briefing slides presented at the Association of the United States Army Symposium and Exhibition, "The Role of Special Operations Forces in Information Operations" Pinehurst, N.C., April 8, 1998.

22. This basic information system typology was created for use in this paper. A weakness found in information operations literature is the lack of a standard model. Another method of analysis utilizes information processing based on the OODA loop concept for offensive and defensive information operations. See Major T. Eipp, *A Concept for Information Operations* (Concepts Division, Marine Corps Combat Development Command, 15 May 1998). Access at http://138.156.107.3/concepts/home.htm.

23. Associated Press, reporting from Fort Worth, Texas, Thursday, June 25, 1998.

24. On a daily basis, information attacks are becoming more common. In late May, hackers hit U.S. Army computers and altered a command's Web site. Before that, India's national security computer network was raided for nuclear weapons secrets. The FBI has reported that from February to June half a dozen substantial attacks have taken place in the United States. See "Hackers Hit U.S. Military Computers," Associated Press, June 6, 1998; and Patrick Connole, "FBI unit reports 'substantial' cyber attacks," Reuters, June 11, 1998.

25. This example is at the binary level. Others examples of data and information alteration include video morphing, voice cloning, and e-mail spoofing.

26. With regard to some of the ethical and conceptual problems involved in information operations, see Bradley Graham, "Authorities Struggle to Write the Rules of Cyberwar: Consequences of Using Computers as Weapons Are Largely Unexamined," *Washington Post*, Wednesday, July 8, 1998, p. A1.

27. Matrixing the information/information system typology used in this paper with the INSCOM model represents a future avenue of research which is beyond the scope of this paper.

28. George I. Seffers, "Inventor Spawns 'Electronic Ebola' for Info War," *Defense News*, Vol. 13, No. 24. June 15-21, 1998, pp. 1, 27. See also *Army Times*, June 28, 1998, p. 27.

29. Reprinted from MG John D. Thomas, Jr. Commander, USAINSCOM, "Impact of Information Operations for the Force XXI Army," briefing slides (presented at AUSA Symposium, "The Role of Special Operations Forces in Information Operations," April 7, 1998).

30. Joint Chiefs of Staff, *Concept for Future Joint Operations*, p. 33.

31. Ibid., p. 35.

32. Joint Chiefs of Staff, *Joint Vision 2010*. Fort Monroe, Va.: Joint Warfighting Center, July 1996.

33. Daniel M. Verton, "High-tech warriors, high-tech wars: the services extend IT from digital warriors to digital logistics," *Federal Computer Week*, June 29, 1998; and Jason Sherman, "Bulking Down," *Armed Forces Journal International*, Vol. 135. July 1998, pp. 32-35. A controversy concerning proper division size exists. See Richard J. Newman, "Renegades finish last: A colonel's innovative ideas don't sit well with the brass," *U.S. News & World Report*, July 28, 1997, p. 35.

34. "Washington Watch: Army will fix computer problems." *AUSA News*, June 1998, p. 21.

35. John E. Greenwood, "Editorial: Coping with Urban Crises," *Marine Corps Gazette*, Vol. 82., No. 6. June 1998, p. 2.

36. See Pascale Combelles Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (Washington, D.C.: DoD Command and Control Research Program [CCRP], Institute for National Strategic Studies, National Defense University, January 1998).

37. Quote attributed to MG Michael W. Ackerman, USA, Chief of Signal. See Jim Tice, "Sending the Right Signal/Information as a Weapon," *Army Times*, May 18, 1998.

38. George Cahlink, "Army After Next Will Rely on More Commercial Technology," *Defense Daily*, June 30, 1998.

39. Editorial, "Two-War Strategy? Modernize, Expand or Give Up," *Aviation Week and Space Technology*, June 29, 1998, p. 70.

40. Besides cost concerns, technical considerations exist. As an example, the Force XXI Battle Command, Brigade and Below ($FBCB^2$) system may not be operational in time for the fielding of the 4th Infantry Division as the First Digitized Division, in Fiscal Year (FY) 2000. See Bryan Bender, "Tests May Delay Fielding of First US Digitised Force," *Jane's Defence Weekly*, July 8, 1998.

41. "Weapons of mass disruption" is an advanced battlespace term based upon bond-relationship targeting considerations. Traditionalists who see this threat view a potential cyber attack as a weapon of mass destruction, which is an inaccurate definition. See George I. Seffers, "NSA Chief Ups Info War Ante: Says Cyber Attack on U.S. is Weapon of Mass Destruction," *Defense News*, Vol. 13. June 29-July 5, 1998, pp. 1, 36.

42. The Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: U.S. Government Printing Office, October 1997).

43. David S. Alberts, *The Unintended Consequences of Information Age Technologies* (Washington, D.C.: The Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, April 1996), pp. 27-28.

44. For the primary references to these examples, see Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington, D.C.: The Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, January 1998), pp. 3-5.

45. Robert J. Bunker, "Higher Dimensional Warfighting: Bond-Relationship Targeting and Cybershielding." *Parameters*. Draft under consideration.

46. Business Editors, "U.S. Army Selects Internet Security Systems' Intrusion Detection Technology to Protect Critical Networked Information," *Business Wire*, July 7, 1998.

47. It has been stated that the Longbow Apache has been designed and built for the digital age. The AH-64A fleet came into being in FY 1984. The AH-64D Modernization began delivery in 1997. The Apache attack helicopter is a transitional system which was conceived during the Cold War and has now been upgraded. See "News Call: The Longbow Apache Introduces the Army's Digital Age," *ARMY*, June 1998, p. 57; and McDonnell Douglas Helicopter Systems, *Team Apache Modernization: Lifting the Fog of War*, Pamphlet, (Mesa, Ariz.: Undated).

48. This would mean that speed and precision would be considered the dominant characteristics of future warfare. These mechanical perceptions are in variance with emergent nonlinear/post-mechanical sciences.

49. Part of this perceptional shift may include Army XXI warfighting doctrine focusing upon who is the "right" enemy. See Dubik, *Creating Combat Power for the 21st Century*, p. 7.

50. A number of visions concerning this battlefield are discussed in the papers delivered at the U.S. Army War College Ninth Annual Strategy Conference, "Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?" March 31 – April 2, 1998. Go to the Strategic Studies Institute (SSI) Homepage at http://carlisle- www.army.mil/ usassi/welcome.htm for further information.

51. In regard to proposed small arms capabilities, see Robert I. Widder, ed., *Report on the Results of the Future Small Arms Conclave "Blue Sky" – 2020*, Contract No. DAAL03-91-C-0034 (Arlington, Va.: Battelle Crystal City Operations 9-10 September 1997). This conference took place at Picatinny Arsenal, N.J., under the sponsorship of the Joint Service Small Arms Program (JSSAP).

52. Derived from "Module 6: IW Weapons" of the U.S. Army War College Information Warfare Tutorial. Posted by the Knowledge Engineering Group (KEG), Center for Strategic Leadership. This module and the tutorial itself can be accessed at: http://carlisle-www.army.mil/usacsl/org/iw/tutorial/intro.htm. It is a condensation of material presented through an advanced course dedicated to Information Warfare taught by NSA Visiting Professor, Mr. Robert J. Minehart, Jr. The tutorial represents an unclassified version of the advanced course. (Notice: Due to the sensitive nature of this section the terms presented are proposed by open source [nongovernmental] authors. The examples offered should be considered only as concepts to stimulate your thoughts on "what-if" possibilities. This presentation neither confirms nor denies the existence of such weapons!)