OPINION PAPER

Is The IW Paradigm Outdated? A Discussion of U.S. IW Theory

Timothy L. Thomas

** The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

Foreign Military Studies Office
Fort Leavenworth, Kansas
E-mail: thomast@leavenworth.army.mil

Abstract

The term information war (IW) helped describe one aspect of the unfolding revolution in military affairs in the 1990s. Today, technological developments are integrating the data processing capabilities of machines and the mind in ways not possible a decade ago. As a result, the old IW paradigm may no longer be applicable, making other potential paradigms and terms worthy of consideration. As the future unfolds, it will be interesting to see if Pentagon theorists use IW or a new term to express a threat to the security of the country, a category of warfare, a method of defense or influence, or leave the concept alone as a conceptual umbrella for a host of terms. Or, will the Pentagon simply update IW theory, perhaps developing Information Peace or Mind-Machine concepts that complement IW?

Introduction

Many military analysts believe the end of the Cold War signaled the close of the age of conventional weaponry. At this juncture, a switch was made to acquire weaponry based on technological achievements spawned by the so-called revolution in military affairs. This latter concept had been under consideration for several years. As one analyst noted

Future historians might well cite the years 1993 and 1994 as the period during which the US military and associated national defense organizations identified Information Warfare as a conceptual vehicle for transitioning from the precepts of the Cold War into the new global realities of the Information Age. This concept is gaining momentum throughout the national security community at a breakneck pace. (Berkowitz, 1997, pp. 175-190.)

American industry and business were the first organizations to fully embrace the power of information-age technologies, and the military soon followed. The Internet as we know it was a military research project to develop redundant communications paths that would work if some communications nodes were destroyed. The Defense Department learned to utilize these technologies in logistics and administrative endeavors, and created attack and defend weaponry that could process information quicker and with greater precision than could its adversaries. The overwhelming effectiveness of this ability was most decisively demonstrated

ISSN 1445-3312 print/ISSN 1445-3347 online

for the first time during the Gulf War. The coalition victory over Iraq was labeled as the first battlefield reliance on information technologies to achieve victory.

US military theorists attempted to describe this new emphasis on technology under the cover of a joint doctrine, Joint Publication 3-13, "Joint Doctrine for Information Operations." (DoD, 1998). Also discussed in the same volume was information warfare (IW). These concepts were new and as a result loosely defined, not completely mirroring the terms that composed them. Those responsible for defining the terms were stepping into totally unmapped territory, and had no frame of reference from which to work other than the existing doctrines of psychological operations (PSYOP), operational security (OPSEC), military deception, and similar related topics. Their work was admirable. IO and IW were used as metaphors to express the technological transformation that was underway in times of peace and conflict, respectively.

Recently, however, conceptual writers working on IW doctrine have adopted some radical changes. Most important for purposes of this article is that IW has been removed from the Army's information-related terminology. The familiar term "information operations" now serves all functions associated with information age processes and weaponry. Such a radical move indicates that the time is ripe for a review of some of the other concepts associated with information operations as well. As the analysis below demonstrates, some of the vital terms around which IO has been constructed remain loosely defined; some international terms that might support IO theory are totally absent from consideration in the US lexicon; and some new paradigms describing the information age are beginning to appear. This article makes several recommendations to tighten up terminology, especially concepts such as information superiority, and focuses squarely on other potential paradigms for interpreting current and future developments, offering one paradigm for discussion.

Terminology and the IO/IW Paradigm: The Early Decisions

An authoritative definition of IO and IW reasonably should encompass the accepted meanings of three components: information, operations, and war. When the terms in JP 3-13 are examined, however, disconnects become apparent regarding how military analysts defined the terms some ten years ago, and how they could have defined them. The old definitions worked because they were new and no one REALLY understood what the terms meant. After thousands of pages have been written on IO and IW, it is useful to quickly review these definitions, pointing out their deficiencies that were not apparent at the time.

Three authoritative sources are used here to examine the definitions of information, operations, and war. The three sources are Webster's Dictionary, the Department of Defense's Dictionary of Military and Associated Terms (DoD, 2001), and Joint Doctrine for Information Operations (DoD, 1998). The reason for using a source outside of the military realm is obvious upon closer examination: first, one of the three terms (war) under discussion *is not defined in either JP 1-02 or JP 3-13*, and therefore Webster's is necessary. Secondly, Webster's dictionary is a generally accepted source while both JP's contain military related terminology that is not generally accepted by the academic community at large. The JPs have not been reconciled with general sources; rather words are defined from a military paradigm and may not mean what someone outside the military thinks they mean.

The two primary definitions for the word "information" found in Joint Publication 1-02 are facts, data, or instructions in any form," and "the meaning that a human assigns to data by means of the known conventions used in their representation." (DoD, 2001, p. 254) JP 1-02 defines an operation as military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense and maneuvers needed to gain the objectives of any battle or campaign.” (DoD, 2001, p. 384)

It would appear, based on a look at these definitions, that IO could have been defined from a purely military point of view in one of three ways. First, as “a military action using facts, data or instructions.” Second, as “carrying out a strategic or tactical military mission using facts, data or instructions.” Finally, as “the process of carrying on combat, including attack and defense means, to gain the objectives of any battle or campaign using facts, data, or instructions.” Joint Publications 1-02 and 3-13 define IO as “actions taken to affect adversary information and information systems while defending one’s own information and information systems.” These official definitions mirror the potential definitions suggested above in a tangential manner. The official definition’s focus is clearly on the information systems of equipment, and not on mental perception or reaction, a huge component of IO, or on facts, data or instruction. The gamut is insufficient to clearly define IO. The Army’s relatively new Field Manual 3.0, Operations, describes the attainment of information superiority (the goal of IO) as capable of putting disparity in the enemy commander’s mind between reality and his perception of reality. (Department of the Army, 2001) It thus discusses influencing the mind of the commander, giving more attention to PSYOP than did the old definitions of IO that relate primarily to equipment and give scant reference to the mind.

Similarly, IW could have been defined differently than it was in JP 3-13 and JP 1-02. War is defined by Webster′s dictionary as a state of usually open and declared armed hostile conflict between states or nations.” (Websters, 1998) JP 1-02 *does not define war*. This is an interesting point. How can one possibly define IW if we do not define “war”? The question is worth asking, for avoidance of controversy is hardly an acceptable price for lack of clarity. This can become a troubling condition. For example, consider the emphasis we put on the correct determination of an “objective” or a “center of gravity” as operational or strategic principles. If we do not define the terms properly, can we make the proper determination? Was a weak definition the reason that IW is no longer in the US army’s lexicon? If so, we will need to inform the international military community (coalition forces that support us), because they are still using the IW phraseology.

JP 1-02 defines IW as “information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.” The latter part of this definition sounds more like the definition of an operation, in that an operation carries on combat to “gain the objectives of any battle or campaign.” Further, the definition of war can only be inferred to mean “crisis or conflict” based on the definition of IW in JP 1-02. That is the only difference between IO and IW.

This problem is exacerbated when foreign concepts are bumped up against U.S. concepts. For example, the 1986 *Russian Military Encyclopedia* (SME) defined military information (there was no entry for information) as “information of a military nature, as well as the process of transmission and receiving of such information.” (SME, 1986, p. 294) An operation was defined by the encyclopedia as “an aggregate of battles, engagements, strikes and maneuvers, coordinated and interlinked in objective, tasks, place and time, by various force organizations, conducted simultaneously and sequentially according to a common concept and plan, to accomplish missions in a theater of operations, a strategic or operational sector, or within a specified period of time; a form of military operations.” (Akhromeev, 1986, pp.

514-515) War was defined as “a sociopolitical phenomenon, continuation of politics by violent means…armed struggle comprises the specific content of war.” (Akhromeev, 1986, p.151).

If the definition of war as found in Webster’s dictionary (JP 1-02 cannot be used since it does not define war) is combined with the definition of information from JP 1-02, then a sample definition of IW could be “open and declared armed hostile conflict between states or nations using data, facts or instructions in any form.” This definition makes little sense. A more appropriate but still imprecise definition would have been “open and declared armed hostile conflict by nations or states that utilizes information or information-based systems and processes to attack human or system processors.”

Even more to the point, information does not actually go to war against other information, further casting doubt on the idea of IW. Data or electron streams can be directed against one another to collide or interfere or influence movement, but they are not in open and declared “armed conflict.” Electrons might collide with other electrons, laser beams may try to destroy computer chips, and directed energy beams may try to destroy satellites. But this is not “IW.” Perhaps it could be called beam confrontation, or electron stream conflict where computer chips and other data-processing elements are the objectives of attack. However, as noted above, this is a mute point. The US army no longer has IW in its lexicon, although it does remain in the digital version of JP 1-02.

Other information-related terms

There are several nations, such as Russia and China that define other information-related issues. These include terms such as information weapons and information-psychological actions. JP 1-02 and JP 3-13 do not define an information weapon, just as they do not define war. There appears to be a long-term unwritten policy in military circles in the US not to define an information weapon. Yet much of today’s weaponry is loaded with computer chips and other information technology, the cornerstones of the information age. The Russians define information weapons in great depth and specificity. They ask “how can you have an information war if you do not have information weapons?” Can we have tank warfare without tanks? This term and others might be worthy of future consideration by IO specialists in this country. One of the greatest strengths of the US armed forces is its ability to learn from other armed forces (for example, the US studied and then adapted the term operational art from Soviet theoreticians). Perhaps now is the time to data-mine foreign IO theory for some of the good ideas that they have developed, and see if they are applicable to the US paradigm.

For example, it is interesting to ask, some ten years down the road, why did US theorists, at the height of peace operations theory at the end of the Cold War, develop the concept of IW instead of “information peace”? That is, how nations might use information technology to prevent conflict. Why did we choose information war? The Soviet threat had evaporated, and a worldwide scare generated by a new term, IW, was the last thing Russian reformers needed. Many in Russia interpreted the term as a method of mind control. Now, however, the time appears right for cogent arguments to be advanced to reject or modify some terms and concepts, and to promote new conceptual vehicles.

And there are terms in the US IO lexicon that could stand a scrub. One of the most important is information superiority (IS). JP 1-02 defines IS as “that degree of dominance in the information domain which permits the conduct of operations without effective opposition.”

(DoD, 2001, p. 255). JP 3-13 defines IS 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”. (JP 3-13, 1998) Most recently The Department of the Army (2001, p11.2) defined information superiority as “the operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.”(Department of the Army, 2001) If anyone reading this or any other article collects, processes, and disseminates the information therein, they do not necessarily have information superiority. What if all of the information in this essay is misinformation? That does not provide information superiority, only information inferiority. To process is not to analyze. Or is it? One argument is that “process” is part of the intelligence cycle: converting raw data to a form that is usable by an analyst or for immediate action by a commander. That is, it hasn’t been analyzed yet. It is only “useable” by an analyst. Another argument would indicate that analyze might be included in the term “process.” The word “information-based processes” in JP 3-13 includes the term analysis (“processes that collect, analyze, and disseminate information using any medium or form”), making it appear that JP 3-13’s authors do not make as big a distinction between process and analysis as might be implied. Perhaps too big a deal is being made of this slight oversight, but it would be nice to add the “reminder” word analysis to the IS definition.

The reason for such reminders is that processing and not analyzing information caused a huge waste of munitions during the air war over Kosovo as fighter pilots targeted mockups that appeared to be real targets. How else can one ascribe the difference in the number of tanks we thought we had “killed” in July of 1999 (according to General Wesley Clark, 110) and the final tallies, some of which ranged as low as 26 tanks? And this occurred in the face of near total information superiority when no air force was flying against ours and we owned the airwaves! The US had “self-deceiving information superiority” as a result. FM 3.0 describes information superiority as “when commanders synchronize all three contributors (intelligence/ surveillance/ reconnaissance, information management, and information operations) and it is greater than the enemy’s.” (Department of the Army, p11-2, 2001) This descriptor considers that information has been processed and analyzed, one hopes, in order to attain information superiority.

One is left with the feeling that IW and some other information-related terms do not exist in a pure state but are simply metaphors for expressing aspects of war using high technology weapons or computers, and to a lesser extent terms associated with psychological operations. But terminology is not the only concern with the old model that has served us so well for ten years.

IO applies to no specific or conceptual model (conventional, non-traditional, etc.) but instead conjures up a unique mental model composed of many elements that exist independent from other forms of warfare. FM 3.0, Operations (Department of the Army, 2001) lists ten different “elements” of IO: military deception; counter deception; operations security; electronic warfare (e-attack, protection, support); information assurance; physical destruction; psychological operations; counterpropaganda; counterintelligence; and computer network attack and defense. Such a broad definition makes it hard to distinguish what IO is not, not what it is! Further, if IO’s goal is to produce a disparity in the enemy commander’s mind between reality and the perception of reality in order to disrupt the ability to exercise C2, as FM 3.0 notes, then IO is really nothing new. Deception has been doing this for years. The methods are the same, but the means (sensors, satellites, holograms, etc.) are different as well as the precision and speed of destruction involved. But IO is something new. Today weaponry does more than just disrupt the ability to conduct C2 via deception or PSYOP. Now weaponry can shut down the data processors of both weapons (computer chips) and the mind (neurons). There is more at stake than just deception.

In its purest form, attacks with electrons or leaflets or other means attack equipment and weaponry on the one hand, but also can attack the logic and decision-making capability of the commander on the other, according to Army FM 3.0. That is, there is a huge psychological warfare component of IO, much greater than is generally implied or discussed. There are information operations against the brain on a daily basis in nations worldwide, especially in advertising and the mass media, where the goal is to influence or persuade through pure influence, debates and tests of logic. Less considered is the more sinister form of an information operation against the brain that uses acoustics or other devices to shut down the normal processing of the brain, much like a laser tries to destroy computer chips. U.S. specialists tend to put these operations out of the IO fold and into a field known as non-lethal operations. Most definitions of PSYOP are all about the first, or soft, use of IO: to influence the logic in someone else's head (leaflets, loudspeakers, deception, etc.), or to use counterpropaganda as an element of defensive PSYOP. Soft PSYOP, however, is not the same as protecting the neurons in your head from being fried by a non-lethal device. Data attacks a human's logic in a soft IO PSYOP attack, and electronic or non-lethal streams of data attack neurons in the brain in a hard IO PSYOP attack. Lasers do the same to computer chips, but the latter is more easily identifiable with IO (physical destruction). What about mental destruction?

In summary, the theories of IO and IW have served the US well for the past ten years. They have given us a conceptual model through which to understand the changes that new technologies have brought us. This paradigm made sense ten years ago. But already, new models and concepts are emerging: Network-Centric War, effects-based strategies, asymmetric war, and operational prototyping are but a few of them. Some of these, based on the discussion above, most likely are already deficient since we have no definition of war! Others are being subsumed under the IO mantle.

Yet another model or paradigm, human and equipment data processors, is offered now for your consideration. It attempts to capture much of the discussion above in a simpler form and under an old term, data processing.

"Data processing Operations:"
Another way to think about the Information Age

The manipulation of data (information) has played an important role throughout the history of armed warfare. Before the creation of the computer chip (a data-processor), an information operation meant influencing or manipulating the actions of the decision-maker, the human. It was more of a psychological operation than an information operation, since there was a heavy reliance on intimidation and deception. In reality, the attack was on a human's logic or on the emotion of fear. Just as today, data (leaflets, messages, newspapers, etc.) or activities (a show of force, atrocities, etc.) were the means to manipulate the data processor known as the mind via deception or intimidation. The transmission of data was slow in ancient times, and this also affected the manner in which data was analyzed.

Today, data processors in weapon systems have provided for a vast improvement in the acquisition and transmission of information, ensuring quick and precise attacks on targets even from standoff positions. Data processors allow commanders to mass effects quickly and precisely at decisive points across broad geographical areas. However, feeding false information into the data processor can still fool the logic of even a computer chip. Wrong information in, wrong information out. A computer chip does not have the ability to "fear" data, but can be programmed to reject certain kinds of data.

Data processors form the core element, the heart if you will, of sensors, satellites, and computers. Thus, computer network operations (CNA, CND, and more recently computer network exploitation or CNE), or attacks on sensors or satellites, are in reality attacks against data processors. In like manner, psychological operations, deception, and even non-lethal operations are directed against the data processor known as the mind. PSYOP and deception have reached new levels of maturity, in that holograms, morphed images, and other virtual representations of reality now have the potential to influence people like leaflets and loudspeakers once did. Non-lethal weaponry, such as acoustics or stun guns, is capable of momentarily shutting down the data processor known as the brain. Non-lethals can be described as soft influence means (leaflets, soft attacks) or incapacitating and even debilitating (hard attack) means. Unfortunately, this important latter attack method is not covered by present day IO theory in the US, which is focused on systems and equipment. 'Non-lethals' are in a separate category for analysis.

People have ignored the fact that the mind has no firewall for too long (although any non-lethal specialist would argue this fact—here IO specialists are addressed!). The primary emphasis on networks and pieces of equipment missed the most exposed computer/data-processor on the battlefield, the human head. PSYOP and military deception are the only elements of those ascribed to IO that are concerned with the human information security feature, logic. A non-lethal substance is much more insidious—it attempts to alter or destroy the functioning of the brain's neurons just as an electron stream or laser beam attacks the data-processor known as the computer chip.

Further, in a recent interview with Wired magazine, Mr. Andrew Marshall of the Net Assessment Office of the Pentagon, often referred to by Pentagon insiders as Yoda, underscored the importance of the mind and its implications for future warfare scenarios. He noted that

People who are connected with neural pharmacology tell me that new classes of drugs will be available relatively shortly, certainly within the decade. These drugs are just like natural chemicals inside people, only with behavior-modifying and performance-enhancing characteristics. McGray (2003, p.117) joked that a future intelligence problem is going to be knowing what drugs the other guys are on.

Thus the data processor, possessed by both equipment (computer chips) and humans (neurons), is the actual center of gravity of future attacks. It might be soft attacks on logic or hard attacks on chips or neurons. The old IO/IW paradigm did not focus on the data processor as the objective of an attack, but rather offered elements and other descriptive criteria to describe IO. However, much of the problem with data processors is related to our reluctance to view a human as a data processor. We are not accustomed to doing so, and don't feel comfortable putting non-lethals into the IO lexicon as a result. Physical destruction appears to have a comfort level of acceptance, but mental destruction does not.

Further, the human is always the interface between the input and output of data processing. The mind must not only ward off deception and acoustic attacks against it, it must also interpret what is downloaded from a computer or satellite, and what is acquired by counterintelligence means (for example, counter EW or HUMINT operations) or developed via counterpropaganda operations. Equipment can produce false outputs that the human interface must be coy enough to process, analyze, and interpret. Once again, the focus is on a human's ability to use proper logic to come to the correct conclusion. The computer-operator or machine-mind interface is one of those centers of gravity for the technological age that people seldom mention. The journal *Technology Review* recently wrote about this development, noting that efforts to link brains and computers could result in thought-controlled robots, enhanced perception and communications, and might make you smarter. (Technology Review, 2003)

Websters (1988) dictionary defines data-processing as the converting of raw data to machine-readable form and its subsequent processing (as storing, updating, combining, rearranging, or printing out) by a computer." The online *American Heritage Dictionary* defines a data processor as a device that performs operations on data; a machine for performing calculations automatically; or a person who processes data. JP 1-02 does not define data processing. This is not surprising since it is not a military specific term, although military forces in almost every aspect of their day-to-day lives (like civilians everywhere) and wartime activities use its capabilities.

Knocking out or manipulating the organizer and distributor of data, the data processor, is the focus of the new paradigm. The data processor is the objective. As a result, it would be more correct to position data-processor wars at the top of the hierarchy of the concept and to position information as a sub-element, a means to influence the data processor. *Attacks on computers or the mind, whether electronic, laser, or other, are designed not to attack information but rather to disable, manipulate or destroy the data processor*. In the case of a sensor, satellite, electronic warfare platform, or a computer, it is an attack on 1's and 0's of computer-based language, or on the computer chip itself. With regards to humans, special light or TV frequencies that induce photoelectric epilepsy, or other forms of debilitating light that attack the actual functioning of a human's data processor, the brain, are the areas of concern. Finally, regarding persuasion management or deception activities, these can be used against either equipment or a human.

If data-processing operations were broken down into two categories, equipment and the brain, what shape would the categories take? If one were to look at the elements listed in FM 3.0, psychological operations, military deception, counter deception, counterpropaganda, and counterintelligence would be listed under the brain as elements designed to influence this data-processor. Non-lethals, not one of the elements in FM 3.0 (Department of the Army, 2001) would also have to be added to the list, since they can shut down both logic and bodily functions. With regards to equipment, electronic warfare, information assurance, and computer network operations (CNA, CND, and CNE) would be listed. Of course, military deception is not purely a function of the human side of the equation. Military deception could be used against a piece of equipment's data processor just as easily as it could be used against a human. A sensor that is fed false signals is one example. Physical destruction and operations security also could fit both the equipment and brain categories.

Are there other paradigms besides data-processing? Of course there are, and several were already listed. The one offered here is just a simple example, and far from the most creative. Most paradigms are susceptible to the same problems as IO and IW, however. They have to be properly defined, meaning they should not offend more traditionally accepted definitions but adapt to them. And care must be taken not to insist on mutually exclusive categories, as IO and IW do. Another suggestion is to divide the conceptual model to describe technological change into three parts: kinetic warfare, electro-magnetic spectrum energy warfare, and PSYWAR (or influence war). Each would have specific sub elements (deception, operational security, etc.). Or one could look at the technological revolution as simply dividing the pie into technology and psychological sectors. In any event, much conceptual thought is needed. Data processing is only a way to think about the problem, not a way to define it. And particularly with regard to non-lethals, there are a whole host of international laws that would affect the development of any mind-related concept.

Conclusions

The rapid pace of development in today's technology sphere indicates that the concept of "information warfare" that served a purpose for ten years is now somewhat dated, or at least in need of updating. IO begins before a crisis or conflict begins and is ongoing during the conflict. To say that military deception, OPSEC, PSYOP (look at the US use of leaflets and TV/radio today to influence the Iraqi population and soldiers long before actual conflict), and other elements of IO only occur during conflict is missing the point. It will be interesting to see if Pentagon theorists use IO to express a threat to the security of the country, a category of warfare, a method of defense, or leave it as the same conceptual umbrella for a host of operations, the function it served in the past. Or will a new prism of analysis replace IO itself?

Elements of the old metaphor are still applicable but a new conceptual model is needed, and especially one with more focus on the mind. The old concepts of IO/IW looked almost exclusively at equipment and systems, and gave scant notice to the mind except for soft PSYOP—counter deception, counter propaganda, military deception, and operational security. But, as pointed out in the text above, the focus was purely on how to influence the behavior and opinions of others, which does not concentrate on protecting the mind from either information that could influence behavior or attitudes, or from weaponry that could upset the functioning of the brain's neurons. One way to prevent such attacks from ever occurring is, again, to ensure international laws are in place to thwart such potential applications.

To underscore future developments regarding the mind, one needs look no further than the August edition of *Newsweek*. (Newsweek, 2002) Inventor Woody Norris indicated that a device he created could now put words or images in your head from 100 yards away. The military and law enforcement officials are closely monitoring the results of this experimentation. This development, if it turns out to work, would further emphasize the importance of protecting the mind. Just as data can be fed into a computer, Norris's invention would indicate that data can be fed into a person's mind as well. The *New York Times, Popular Science,* and *Business Week* followed up with stories on Norris's invention a few months after the *Newsweek* article.

A clear future problem will be not only validating concepts in the US, but attempting to get nations across the globe to find a common language if/when the problem of IO/IW is brought before the United Nations. Just because we "invented" IW and the Army has now discarded it does not necessarily mean that other nations will do the same. One Chinese officer, for example, noted that IW is ongoing all the time, and IO only happens in wartime. A key Russian concept, around which that country has developed a doctrine and policy, is "information security." Both nations define information weapons. All of these approaches are not explored fully in current US thinking. Of course, US policy makers have consciously decided to ignore some of these concepts for national security reasons, and their concerns are real.

It is unfortunate that the focus of defense departments worldwide is so focused on IO or IW and not on “virtual peacemaking” or “information peace” concepts. Information technologies were used extensively to keep the sides from fighting after US forces entered Bosnia, and a precedent was set. The presidents of Serbia, Croatia, and Bosnia-Herzegovina were influenced strongly by the use of information technology to come to a common agreement when their borders were divided. At Dayton, the presidents were placed in a room and shown a virtual flyover of crucial border regions. From information in the video, they were able to discuss and develop among them solutions to sensitive issues. Such use must be at the forefront of our efforts, not the afterthought.

In Iraq, information technologies were used to ascertain if the US and other nations would eventually go to war. No one is talking about the UN’s use of high technology as a “virtual peacemaking” or “information peace enforcement” operation. Rather, people only are thinking of IO use in a conflict. More attention needs to be focused on the persuasive influence of high technology developments, and not just by the Pentagon. The State Department should be in the lead on this issue. They have developed a good grasp of virtual diplomacy issues, and need to continue to push such agendas and methods for resolving issues via negotiations.

One conceptual paradigm offered here was the data-processing model. And that was all it was, a potential concept. Others are certainly available and should be analyzed. IO, as a result, may be the victim of the next mental scrub over future developments. Whatever model is chosen, it must be simplistic, reflect reality and offer a way for thinking about the evolving nature of the world around us. IO and IW were excellent starters that helped military people understand the changing nature of technology. Now might be the time to move on to other concepts, or to slightly alter the initial IO and IW concepts. Contemporary developments will soon mimic some of the futuristic scenarios that Hollywood filmmakers are portraying (*Minority Report* comes to mind immediately)—and we will need a paradigm from which to understand them.

References

Akhromeev,S.F (1986) *Russian Military Encyclopedia*, Second Edition, Moscow.

Berkowitz, B.(1997) Warfare in the Information Age. *In Athena’s Camp*, eds: J.Arquilla, D. Ronfeldt, National Defense Research Institute, RAND, Santa Monica.

Department of the Army (2001) _*FM 3.0, Operations*, Headquarters, Department of the Army, U.S. Army Printing Agency, Washington, D.C.

DoD (2001) *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 21 April 2001. URL: http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf .Accessed on 7 May 2003.

DoD (1998) *Joint Publication 3-13: Joint Doctrine for Information Operations*, 8 October 1998

Huang, G. (2003) Mind-Machine Merger, *Technology Review*, May 2003.

McGray, D. (2003) The Marshall Plan. *Wired Magazine*, Issue 02/2003

Reno, J., Croal N. (2002 Hearing is Believing, *Newsweek*, 5 August 2002, Internet version.

Websters (1998) *Merriam-Webster's Collegiate Dictionary*, Tenth Edition, Merriam-Webster, Incorporated, Springfield, Massachusetts, U.S.A., , p. 599.