George J. Stein

Information Warfare: Words Matter

Introduction

The terminological basis for any discussion of Information Warfare (InfoWar) must be found in the "real world" rather than philosophical, linguistic or etymological speculation. As interesting as philosophical speculation might be, it must be recognized that "war" and thus, InfoWar, is primarily an act of the State carried out by the armed forces of the State. Of course, "hacking" and other "cyber" activities by teenagers or criminal enterprises against individuals, banks or public utilities could be seen as a kind of "infowar," but, for the purposes of this paper, these are considered "criminal" activities. InfoWar, in this paper, is a State activity carried out, in large part, by the armed forces of the State. Of course, State-directed InfoWar could be conducted by the intelligence or other state-security agencies. However, if Clausewitz was correct and "war is the continuation of [State] policy by other means," then InfoWar must be seen as a new set of "means" to execute State policies.

The current attention to InfoWar is, in large part, consequent of the rather public discussion of the topic by the US military. This paper will show the evolution of the concept of InfoWar in official and semi-official documents published by the US Armed Forces. Special attention will be given to the concepts of InfoWar current in the United States Air Force as, appropriate for the Service most responsible for "strategic" warfare, the USAF has developed the most interesting ideas. The documents to be consulted generally fall under the category "doctrine." For the US Armed Forces, and indeed for any modern military establishment, doctrine comprises not only "how" the forces will fight or conduct other operations such as humanitarian relief, but, more importantly, how the forces will "organize, train and equip" to execute their mission. Again, for the US Armed Forces, doctrine is divided between individual branch of service doctrine and "joint" doctrine. Each branch of service has its own doctrine. How the Army, the Navy and US Marine Corps, and the Air Force plan to fight and "organize, train and equip" are based on the peculiar and unique characteristics of the "realm" (land, sea or aerospace) in which they primarily conduct operations.

In the United States, each of the individual services organize, train and equip to be able to supply forces to the geographically-based Commanders-in-Chief (CinCs) such as European Command (EUCOM) or Pacific Command (PACOM). The services will deploy as services, but "fight" together or "jointly" under a "Joint Force Commander" who will have "command and control" over each individual service. That is, the Army, Navy or Air Force do not go off on their own and conduct their own separate war. As the ability to conduct operations together has become central in the employment of US military forces, "joint" doctrine has evolved in recent years. More importantly, for the US Armed Forces, joint doctrine is authoritative and has precedence over individual service doctrine. In the context of InfoWar, then, a review of the evolution of "official" joint doctrine is the most accurate reflection of the terminological basis of any "real world" discussion or analysis. Again, if "[info]war is the continuation of policy by other means," the InfoWar doctrine of the armed forces of the State is the necessary, but not sufficient, terminological foundation to discuss Information Warfare.

Evolution of InfoWar Terminology

The first official and public recognition by the US Armed Forces appears to have been in the "Memorandum of Policy No.30 (1993): *Command and Control Warfare*."[1] Command and Control Warfare (C2W) was defined as "*the* (emphasis added) military strategy that implements Information Warfare *on the battlefield* (emphasis added) and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of troops." MOP 30 refers the reader to a previous "DOD (Department of Defense) TS (Top Secret) 3600.1 —Information Warfare–1992" (still classified) for a discussion of Information Warfare. Three items are crucial: (1) InfoWar and Command and Control Warfare (C2W) are identified as mutually relevant concepts, (2) this is a very "army" or land-battle view of warfare, and (3) the recent experience of the Gulf War was identified as the essence of C2W. Recall Gen. Colin Powell's comment on defeating the Iraqi military: "first we cut off its head, then we kill it."

Joint Doctrine in the US Armed Forces evolves in a very complex way. In essence, one Service is assigned the "lead" to develop the first draft and then coordinate the comments, assent and dissent, alternative views, etc. of the other Services through the Joint Doctrine Center. The idea, in theory, is to prevent joint doctrine reflecting only the views of one Service. Joint Doctrine is ideally a consensus view. As the various draft versions of joint doctrine for C2W circulated among the Services, the initial view (cited above) was seen as too narrow. Likewise, it was pointless to discuss C2W in a context where the definition of the parent concept, Information Warfare, was still Top Secret. Finally in 1995, many drafts later, the debate and discussion became "Joint Publication 3-13.1–*Joint Doctrine for Command and Control Warfare*." JP 3-13.1 is, then, an authoritative terminological foundation for the discussion of InfoWar in the US Armed Forces–until the "parent" JP 3-13 *Information Operations* (still in draft coordination) is released.[2]

The most significant evolution from MOP 30 to JP 3-13.1 is the recognition that Command and Control Warfare (C2W) is "*an* application of IW *in military operations* (emphasis added)." C2W applies "across the range of military operations and at all levels of conflict." C2W is both offensive and defensive. Doctrine, of course, is written in very terse and condensed style. The implications of a militarily doctrinal statement are left to the reader–militarily sophisticated readers with a range of military and political tacit knowledge. Apart from the obvious need for both defense and offense, a militarily sophisticated reader would imply that while C2W is "an application of IW *in military operations*," (a) there might be other applications of IW in military operations and (b) there might be applications of IW in other than military operations. Likewise, C2W now applies "across the range of military operations and at all levels of conflict." That is, it is not constrained to a simple battlefield objective of disrupting the enemy commander's command and control of his troops. The Joint Doctrine for Command and Control Warfare, then, is probably the best window through which to observe the evolution of InfoWar. Joint Doctrine for C2W will guide each of the individual Services as they "organize, train and equip."

Two key definitions from JP 3-13.1:

Command and Control Warfare (C2W) is "the integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions."

Information Warfare is publicly identified as "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems and computer-based networks while defending one's own…"

Key issues to note include:

C2W is distinctive only in that it is the "integrated" use of five already existing sets of "organized, trained and equipped" military capabilities. C2W is a *new way* to think about and employ traditional military functions such as electronic warfare, operations security, etc. C2W is not so much technologically dependent as it is an ability to "integrate" assets to "deny information to, influence, degrade, or destroy adversary C2 capabilities." C2W is a *way* of fighting, not a technology of fighting. It is not just about "cyber" or computer-based combat.

InfoWar, while militarily relevant, is clearly recognized as a much larger concept. While the armed forces are capable of contributing expertise, equipment or personnel to "actions taken to achieve information superiority… ," it is not asserted that InfoWar is either a central military mission or that the Armed Forces even have a primary role.

This, in my opinion, is the central reason that discussions by the US Armed Forces since 1997 have begun to shift away from the phrase "Information Warfare" to the much less ominous sounding "information operations." Thus, the draft "parent" JP 3-13 *Information Warfare* in circulation for coordination has already been transformed into *Information Operations*.

Joint Pub 3-13.1 remains central to understanding the conceptual and terminological basis of InfoWar as it notes that "effective C2W provides the JFC (Joint Force Commander) the ability to shape the adversary commander's estimate of the situation in the theater of operations." Or, in plain speech, affect the enemy's ability to know what's going on though the integrated use of electronic warfare, deception, etc. Then, in probably the most interesting statement in the whole document, JP 3-13.1 sets out the central goal of C2W -- the Holy Grail of InfoWar. JP 3-13.1 asserts that it "may even be possible to convince the adversary that the US had 'won' prior to engaging in battle, resulting in deterrence and preempting hostilities." This is, of course, the key to the whole discussion. What is implied is that the proper integration of *already existing* military capabilities designed for battlefield "operational" or "tactical" employment can transcend the battlefield to have the "strategic" effect of deterrence or preemption of hostilities. Properly employed, military C2W operations might be seen as a crucial evolution in, what the Tofflers' have called, "anti-war" or the avoidance of "battle."[3] Lest this seem odd, it has been noted in the press by military commanders in the current operations in Bosnia that their "information superiority" and ability to "shape the adversary commander's estimate of the situation" has been the most important "asset" at their disposal to maintain "peace."

More simply stated, the "organization, training and equipment" for C2W can be readily employed by the armed forces for "Information Operations" or, *ceteris paribus*, InfoWar well beyond traditional notions of the decisive engagement. Indeed, it is precisely the potential for Information Operations or InfoWar to be inserted into the seams among the components of the Clausewitzian "remarkable trinity" (*wunderliche Dreifaltigkeit*) of State, armed forces and civil population which raises the question of whether or not InfoWar represents a true "Revolution in Military Affairs." InfoWar can not only separate the commander from his troops, but the State political control from the armed forces or, equally revolutionary, the people from the State.

The US Air Force and InfoWar

The US Air Force has just released its new foundation doctrinal statement: *Air Force Basic Doctrine: Air Force Doctrine Document 1 (September 1997)*.[4] All future USAF doctrine will be derived from *AFDD-1*. As required, *AFDD-1* is fully in conformity with Joint Doctrine but, as in each individual Service, takes an interpretation appropriate to the aerospace realm of warfare through the addition of particular USAF experience and planning. The most important addition in the new basic doctrine is the assertion that "information superiority" has been elevated to an importance equal to the traditional core competencies of air and space superiority. "Dominating the information spectrum is as critical to conflict now as controlling air and space, or *as occupying land was in the past* (emphasis added), and is seen as an indispensable and synergistic component of air and space power." From the perspective of the USAF, as it is the principle supplier and operator of the global air and space reconnaissance, surveillance and intelligence systems, and as the "global reach" provided by both air and space assets permits far more rapid response than traditional terrestrial or maritime forces, it is only natural that "information superiority" becomes coequal with aerospace superiority. Information superiority is, quite frankly, an ambitious goal. On the other hand, it is recognized as the *sine qua non* for contemporary future aerospace employment and, moreover, equally central to the new "operational" (or battlefield) concepts demanded in the "parent" Joint Doctrine, *Joint Vision 2010*, of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[5] For the USAF, Information Superiority is the "ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same." And, like the traditional roles of air and space superiority, includes "gaining control over the information realm (emphasis added) and fully exploiting military information functions." *AFDD-1* accepts and repeats the standard definitions of Command and Control Warfare (C2W) and Information Operations discussed previously. It adds that Information Warfare are Information Operations "conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" and, thus, preserves the recognition that InfoWar is the lesser included case, or subset, of Information Operations.

Doctrine, albeit distinctly directive, is not the only authoritative source to discover the nomenclature and official thinking on US InfoWar. Each of the Services has produced official "think piece" publications to shape the doctrinal, inter-service rivalries, and political debates. The arguments for the resources to "organize, train and equip" and the arguments within a particular Service between traditionalists and innovators are often made through the publications issued over the signature of the (civilian) Secretary of the Air Force and the (military) Chief-of-Staff. For the USAF, the publication issued by the Secretary *and* the Chief-of-Staff, *Cornerstones of Information Warfare*, is the most interesting in that it develops an approach to InfoWar quite distinctive from the more (if one can say) "traditional" approaches to InfoWar of the other Services.[6]

Cornerstones argues, almost counter-intuitively, that InfoWar can be considered as either "indirect" or "direct." Indirect InfoWar is conducted by changing an adversary's information though the creation of phenomena or events which must be observed or perceived by the adversary to be effective. A false radio broadcast not heard by the adversary, or even a false radar image not detected by the enemy air defense system, is a waste of electrons. For the USAF in *Cornerstones*, what the other Services call Command and Control Warfare (C2W) is, at best, indirect InfoWar conducted merely by the "integrated" employment of very traditional military techniques of psychological operations, electronic warfare, deception, etc. Yes, it is InfoWar, it is also just not very new and remains far too dependent on adversary

perceptions and reactions. In essence, the USAF recognizes the reality of the global information infrastructure. Any serious adversary in the future will have access to "infinite" alternative, even multispectral, sources of information against which to cross-check his perceptions. The "CNN effect" and the global infosphere may render traditional means to protect "friendly" information or project false information a waste of scarce resources. For the USAF, it may be best to "organize, train and equip" for "direct" InfoWar.

Direct InfoWar is seen as "changing the adversary's information without involving the intervening perceptive and analytical functions." That is, the information is changed, and presumably acted on, without the adversary even being aware that he has "perceived" the false information. Direct InfoWar would be conducted, most likely, through what *Cornerstones* calls "information attack." That is, "directly corrupting information without visibly changing the physical entity within which it resides." Clearly, inserting a computer virus which could change the algorithms by which an antiaircraft gun plots its fire would meet this definition. That is, the gun's computer continues to hum along nicely–the shells are all just twenty meters too high. How, or even if, such an "information attack" could be made against even so simple a device as an antiaircraft system is, undoubtedly, shrouded in what in the US military calls the "Black World" of highly classified research. That such a capability would be a valuable "direct" InfoWar asset is unarguable. Clearly, affecting the *Weltanschauung* by which the adversary leadership, armed forces or people interpret observed events would be "direct" InfoWar of the most refined and subtle order. That such a capability would be a most valuable "strategic" asset is unarguable.

Fantasy or the Future of War?

While "changing the adversary's information without involving the intervening perceptive and analytical functions" sounds like science-fiction or an old research project by the Soviet KGB on reflexive control, it can be seen as a logical implication of an important "warfare epistemology" shared widely in the US armed forces. The late USAF Col. John Boyd (died 1997) was an expert fighter pilot and, after retirement, strategic thinker who developed an approach to conflict which has become known as the "O-O-D-A Loop" among US military and business strategists.[7] In essence, any conflict situation can be dissected analytically into four components: observation, orientation, decision and action. From fighter pilot to business strategist, first one must perceive accurately the environment. The second phase, "orientation" is the mental process by which the observed is compared/contrasted with the already known. It is what pilots might call "situational awareness" and philosophers, tacit knowledge. On the basis of the "analysis" of the observed with the known, one "decides" and "acts." O-O-D-A. For John Boyd, the goal of the fighter pilot is to "get inside" the adversary's "loop" and either observe, orient/appraise, decide, and act "faster" or more accurately than the adversary. This simple idea has become the "warfare epistemology" very common in US military thinking and dozens of citations in Joint and Service doctrine, training manuals, etc. could be provided easily.[8] It is especially influential in the US Marine Corps. The annoying thing for the researcher is that Boyd's ideas are circulated on the basis of photocopies of slides made from a lecture "Discourse on Winning and Losing" he delivered hundreds of times in the various military service schools and the Pentagon. There is no "in print" version of Boyd's original ideas.

For many in the US military InfoWar community, Information Operations, InfoWar and Command and Control Warfare (C2W) are based directly on the idea that IW or C2W are, in their essence, a means to influence, disrupt, delay, or "get inside" the adversary's O-O-D-A loop or decision cycle. The ultimate or end product of any military operation is some "act."

This "act" is a consequence of the military unit having received an order, or "decision" from higher command. Clearly, if the command and control system is degraded through disruption of the transmission of the "decision" to the "actor," that unit's effectiveness (or better, military relevance) is reduced. So, attack the enemy's communication system. Shoot the carrier pigeon or jam the radio transmission.

Disrupting the links between "decide" and "act" will still be useful and will still be attempted. Standard-brand electronic warfare (EW) will continue. Many military thinkers, especially in the USAF, suspect that the future of the global infosphere, especially the infinitely complex, secure and redundant telecommunication networks, will make any attempt to "shoot the pigeon" a waste of scarce military resources and effort. There will just be too many alternative paths to communicate decisions to subordinates. Likewise, this evolving and planet-wide communications density permits a "distributed" decision-making system which will be more difficult to influence or disrupt. The "indirect" InfoWarrior has a problem.

Recall that the "Holy Grail" of the InfoWarrior is to "to shape the adversary commander's estimate of the situation in the theater of operations" in such a way as to "convince the adversary that the US had 'won' prior to engaging in battle, resulting in deterrence and preempting hostilities." In terms of the military epistemology of the O-O-D-A loop, the InfoWarrior's "target" is all the capabilities, thought processes and actions that allow an adversary to correctly "observe" the battlespace, assess ("orientation") what those observations mean; use this assessment to make timely, accurate and effective "decisions" and communicate these decisions as command and control for effective and timely "actions."

The USAF, on the basis of its familiarity with its global intelligence, reconnaissance, surveillance and communications capabilities, has, as noted above, decided that InfoWar based primarily on attacking the "observation" component of an adversary's O-O-D-A loop may be ever-more difficult and ever less effective. A moment's reflection demonstrates that the traditional components of Command and Control Warfare depend for their effectiveness, for the most part, on the "perception" or "observation" they create. Thus, the USAF in *Cornerstones* called this "indirect" InfoWar as the effect is not produced without the intervening "observation." "Direct" InfoWar, especially that attempted through "information attack," targets the "orientation" component/phase of the O-O-D-A loop.

The real-world targets for a sophisticated InfoWarrior, then, are (conceptually) the "mediators." That is, there is always some process or system, some persons, some machines or technology that translates data (observation) into the information required by decision-makers to orient/assess prior to effective decision-making (command and control). There is someone, something or some way that "mediates" or translates the great buzzing infosphere of data into information for the decision-maker. It might be a physical computer program or it might be the "picture" of US intentions he carries in his head and by which he interprets his observations. From the perspective of an InfoWarrior who accepts the challenge of Direct InfoWar, the most important project and the key assignment to the Intelligence and Analytic Community is to discover and map, logically and empirically, the "mediators." At a minimum, these mediators would include: (a) US, allied and adversary leadership, (b) the civil infrastructure through which information is mediated, (c) the military command and control infrastructure and, finally, (d) the technological, electro-mechanical and digital systems which permit weapon effectiveness.

If the global infosphere increasingly precludes deception, propaganda, and disinformation aimed at creating appropriate "perceptions," the only (logical) basis for InfoWar is to target

the "orientation" by which perception is assessed and evaluated as the basis for decisions. Perhaps the most accurate translation into German is not "Informationkrieg" but, *pace* Hegel, "Geistkrieg."

[1] CJCS, MOP-30–Command and Control Warfare (1993).

[2] Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare*, (1995).

[3] Toffler, Alvin & Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, (NY: Little, Brown & Co., 1993).

[4] Department of the Air Force, *Air Force Doctrine Document 1: Air Force Basic Doctrine*, (September 1997).

[5] CJCS, *Joint Vision 2010*, (1996).

[6] Department of the Air Force, *Cornerstones of Information Warfare*, (n.d.).

[7] while no published work by John Boyd is available, an early and very accurate discussion of his ideas on the O-O-D-A loop can be found in: Orr, George E., *Combat Operations C3I: Fundamentals and Interactions*, (Maxwell AFB, AL: Air University Press, 1983). See also: Stein, George, *US Information Warfare: Jane's Special Report*, (VA: Jane's Information Group, 1996).

[8] See the authoritative, *Joint Vision 2010*.