Search Site: Go
IWS - The Information Warfare Site
Home | Information Operations | Categories | Infocon | Reviews | Forum | News | Mailing Lists | Links | Support IWS
About IWS | Site Map

Published *Airpower Journal* - Spring 1995
DISTRIBUTION A:
Approved for public release; distribution is unlimited.

What is of supreme importance in war is to attack the enemy's strategy.
SUN TZU

INFORMATION WARFARE

Prof George J. Stein, AWC

We need to state up front that much of what is discussed in this essay on information warfare is unofficial speculation. There is no official, open-source US government definition of information warfare. The Department of Defense calls its current thinking and approach to information warfare "command and control warfare" (C2W).[1] There is little agreement among the services about either information warfare or C2W; and among civilian defense analysts looking at the issues of information warfare, there is even less agreement. Why, then, should we be thinking about this new and strange idea? The chief reason, of course, is that while we don't know just what we've got here, all the services agree that information warfare is something important.[2] Was Desert Storm the first war of third-wave information warfare or the last war of mechanized second-wave industrial warfare?[3] We're not sure, but a lot of people, including potential rivals, are trying to figure it out.[4] This article attempts to make some sense of this new idea called information warfare. We'll look at four sets of ideas: (1) A definition of information warfare; (2) How we should start thinking about developing a strategy of information warfare; (3) Why current Air Force doctrine may be the best framework for developing a doctrine of information warfare; and (4) A very brief comment on the danger of failing to develop information warfare.

Defining Information Warfare

Information warfare, in its largest sense, is simply the use of information to achieve our national objectives. Like diplomacy, economic competition, or the use of military force, information in itself is a key aspect of national power and, more importantly, is becoming an increasingly vital national resource that supports diplomacy, economic competition, and the effective employment of military forces. Information warfare in this sense can be seen as societal-level or nation-to-nation conflict waged, in part, through the worldwide internetted and interconnected means of information and communication.[5] What this means is that information warfare, in its most fundamental sense, is the emerging "theater" in which this means is that information warfare, in its most fundamental sense, is the emerging "theater" in which future nation-against-nation conflict at the *strategic* level is most likely to occur. Information warfare is also changing the way theater or operational-level combat and everyday military activities are conducted. Finally, information warfare may be the theater in which "operations other than war" are conducted, especially as it may permit the United States to accomplish some important national security goals without the need for forward-deployed military forces in every corner of the planet. Information warfare, then, may define future warfare or, to put it another way, be the central focus for thinking about conflict in the future.

Information warfare, in its essence, is about *ideas and epistemology*- big words meaning that information warfare is about the way humans think and, more important, the way humans make decisions. And although information warfare would be waged largely, but not entirely, through the communication nets of a society or its military, it is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decisions they make. The greatest single threat faced by the Air Force, and by the services in general, as we begin to think about information warfare is that we will yield to our usual temptation to adopt the new technologies, especially information technologies, as merely force multipliers for the current way we do business.[6] It would be a strategic mistake of historical proportions to focus narrowly on the technologies; force the technologies of information warfare to fit familiar, internally defined models like speed, precision, and lethality; and miss the vision and opportunity for a genuine military revolution. Information warfare is real warfare; it is about using information to create such a mismatch between us and an opponent that, as Sun Tzu would argue, the opponent's *strategy* is defeated before his first forces can be deployed or his first shots fired.

The target of information warfare, then, is the human mind, especially those minds that make the key decisions of war or peace and, from the military perspective, those minds that make the key decisions on if, when, and how to employ the assets and capabilities embedded in their strategic structures. One could argue that certain aspects of the cold war such as Radio Free Europe, Radio Martí, or the US Information Agency were a dress rehearsal for information warfare. One could argue that certain current capabilities in psychological operations (PSYOP), public affairs and civil affairs, together with the intelligence agencies, satellite drivers, communications specialists, computer wizards, and the men and women in agencies like the Air Intelligence Agency or the new Joint Information Warfare Center, represent some of the key learning environments in which we'll develop some of the new capabilities for information warfare.[7] And while the concept of information warfare in its computer, electronic warfare, and communications net version is most familiar in military operations involving traditional state-to-state conflict, there are new and dangerous players in "cyberspace"-the battlefield for information warfare. There has been a proliferation of such players- nonstate political actors such as Greenpeace, Amnesty International, rogue computer hackers like the Legion of Doom, some third world "rebel" who stages a "human rights abuse" for the Cable News Network (CNN), or ideological/religious inspired terrorists with easy access to worldwide computer and communications networks to influence, to exchange information, or to coordinate political action on a global basis. All of this suggests that the military or governments of a traditional nation-state may not be the only serious threat to our security or the driver of our national security politics.[8] Cyberspace may be the new "battlespace," but the battle remains the battle for the mind. There must be no confusion of the battlespace with the battle.

Let's take a look at this in a context we think we're familiar with: propaganda as an effort to influence national morale and support for the nation's armed forces. The Vietnam War taught us the consequences of winning every battle in the field and losing the information war on the home front. Before the advent of information warfare, propaganda was traditionally targeted through various mass media to influence a mass audience. One key change made possible by the new technologies is the potential for customized propaganda. Those who have received individually targeted political advertising from a company specializing in "niche" marketing research must have had a momentary shudder when they realized that there are private companies who seem to know everything about their buying habits and tastes, whether they support the National Rifle Association or attend Tailhook conventions, and what television shows they watch. Every credit card purchase adds data to someone's resources, and not everybody is selling just soap or politicians. Contemporary public and commercial databases and the constantly expanding number of sources, media, and channels for the transmission of information, essentially available to anyone with a bit of money or skill, have created the opportunity and "target sets" for custom-tailored information warfare attacks on, to take just one example, the families of deployed military personnel. Think about the morale implications of that for a minute. Computer bulletin boards, cellular telephones, video cameras, and fax machines-all of these provide entry points and dissemination nets for customized propaganda assaults by our opponents on military, governmental, economic, key civilian strategic structures, or even the home checking accounts of deployed troops.[9] Operations security (OPSEC) is increasingly a most vital military security issue. However, information warfare should not be confused with or limited to just propaganda, deception, or traditional electronic warfare.

A major new factor in information war is the worldwide infosphere of television and broadcast news. Information warfare at the strategic level is the "battle off the battlefield" to shape the political context of the conflict. It will define the new "battlespace." We face an "integrated battlefield," not in the usual sense of having a global positioning system (GPS) receiver in every tank or cockpit but in the Clausewitzian sense that war is being integrated into the political almost simultaneously with the battle. Many people suspect that the national command authorities (NCA) are in danger of becoming increasingly "reactive" to a "fictive" universe created by CNN, its various international competitors, or even a terrorist with a video camera.[10] This media-created universe we live in is fictive rather than "fictional" because although what we see on CNN is "true," it is just not the whole, relevant, or contextual truth. Nevertheless, this fictive universe becomes the politically relevant universe in which the government or the armed forces are supposed to "do something." Members of Congress, the national command authorities, and our mothers all watch the "instant news" followed by "instant" second-guessing commentary. This is increasingly the commander's nightmare. First, 15 congressmen are calling the chairman of the Joint Chiefs to ask whether retired admiral so-and-so's critical analysis on "Nightline" of the CINC's ongoing theater air campaign is valid. More importantly, 300 congressmen are also getting 10,000 calls, E-mails, faxes, and even letters from angry families who've just seen the television report (carefully "leaked" to French television by an unhappy defense contractor and innocently repeated by CNN) that the US military-issue antimalaria pills don't work in Bongo-Bongo. All this without the real "bad guys" trying their hand at information war. Use your imagination. Somalia gets in the news, and we get into Somalia despite the reality of equally disastrous starvation, disorder, and rapine right next door in Sudan. The truth is that there were no reporters with "skylink" in Sudan because the government of Sudan issued no visas to CNN reporters. We all know the impact of the pictures of the failed raid to capture Mohamed Farah Aidid in Somalia. The potential, then, for governments, militaries, parties in a civil war such as Bosnia, or even religious fanatics to manipulate the multimedia, multisource fictive universe of "the battle off the battlefield" for strategic information dominance should be obvious.[11] The armed services are just beginning to think about how these new technologies of instant communication will change the battlespace, and, quite frankly, there are not many good answers yet.

Fictive or fictional operational environments, then, whether mass-targeted or niche-targeted, can be generated, transmitted, distributed, or broadcast by governments or all sorts of players through increasingly diversified networks. The information war potential available to states or other players with access to the universe of internetted communications to use the networks over which banking information is transmitted to suggest that a "hostile" state is about to devalue its currency could easily provoke financial chaos.[12] Direct satellite radio or television broadcasts to selected audiences, analogous to central control of pay-per-view programs, again offers the potential for people in one province or region of a targeted state to discover that the maximum leader has decided to purge soldiers from their clan or tribe from the army. Your own imagination can provide many examples of how the increasingly multisource communications systems offer both the armed forces and the national command authorities countless new possibilities for societal-level information warfare to shape the information battlespace to our advantage.

Let us take just one example of how current technologies could be used for strategic-level information warfare. If, say, the capabilities of already well-known Hollywood technologies to simulate reality were added to our arsenal, a genuinely revolutionary new form of warfare would become possible. Today, the techniques of combining live actors with computer-generated video graphics can easily create a "virtual" news conference, summit meeting, or perhaps even a battle that would exist in "effect" though not in physical fact. Stored video images can be recombined or "morphed" endlessly to produce any effect chosen. This moves well beyond traditional military deception, and now, perhaps, "pictures" will be worth a thousand tanks. Imagine the effect of a nationwide broadcast in banditland of the meeting between the "digitized" maximum leader and a "digitized" Jimmy Carter in which all loyal soldiers are told to cease fighting and return to their homes. The targets of information warfare, remember, are the decisions in the opponent's mind, and the battlespace of the human mind is also the zone of illusion.

Let's play with this a bit. Through hitching a ride on an unsuspecting commercial satellite, a fictive simulation is broadcast. This may not be science fiction, and readers of Tom Clancy's latest novel *Debt of Honor* will suspect it's not. Simultaneously, various "info-niches" in the target state are accessed via the net. Some of the targets receive reinforcement for the fictive simulation; others receive slightly misleading variations of the target state's anticipated responses, and the whole of the opponent's military is subject to a massive electronic deception operation. What is happening here?

At the strategic level, this is the paralysis of the adversary's observation, orientation, decision, action (OODA) loop.[13] The opponent's ability to "observe" is either flooded or very slightly and subtly assaulted by contradictory information and data. More importantly, his ability to "orient" is degraded by the assault on the very possibility of objective reasoning as we replace his "known" universe with our alternative reality. His "decisions" respond increasingly to our fictive or virtual universe, and, most importantly, military "actions" within his strategic structures become increasingly paralyzed as there is no rational relationship of means to ends. What he does is not based on reality because we've changed his reality. This is real war fighting. It would seem, then, that if we can develop a strategic vision and real capability for information warfare, we can bring American strategic power within sight of that elusive "acme of skill" wherein the opponent is subdued without killing as we destroy his ability to form or execute a coherent strategy. How, then, do we think about developing information warfare strategy?

Developing Information Warfare Strategy

Developing a strategy of information warfare starts with serious, creative, and "color-outside-the-lines" thinking about current information technologies and ways in which these might be turned to strategic purpose to serve the national command authorities and military use. This will involve thinking about information in new ways: What information is needed? What organizational changes would occur in the way we gather, process, distribute, and use information? What information-based operational changes could then happen?[14] The services are starting this new thinking under the label "command and control warfare."[15] This, however, is only the first step, as the "digitized battlefield" fails to revolutionize strategic thinking. Let's illustrate this with a bit of history. As Speaker of the House Newt Gingrich observed, some time before the American Civil War, the Prussian general Helmuth von Moltke was thinking about railroads and telegraphs:

> *If we used the telegraph to relay mobilization orders quickly and then used railroads to concentrate troops from bases scattered throughout Prussia, we could concentrate the main effort at the key battle location of a campaign. We wouldn't have to mobilize the army, then concentrate it, then march it to where we hoped the key battle would occur*.[16]

Good insight. And this, unfortunately, is about where we are when we think of information warfare as only command and control warfare.[17] That is, how does this technology permit tanks, ships, and aircraft to do what they do now a bit better. It was Moltke's next insight, argues Speaker Gingrich, that the Joint Staff and the services need to imitate:

> *But the Prussian army is not organized, nor does it operate in a way that would permit it to respond to telegraphed orders to get on trains and show up somewhere else. That's not how we organize, train, and equip. What I need to do is reform the way to get the information needed to*
>
> *do this, the way we're organized so we can use this information, and figure-out new ways to operate; what I need is a new General Staff system*.[18]

So Count von Moltke realized that before he could make revolutionary use of the new technology, he had to solve the higher-order question of what changes in information, organization, and operations would be needed. This is the challenge we face now. The armed forces have a good idea that information technologies just might be the driver in future warfare, but we haven't yet articulated the strategic vision or identified the higher-order changes we need to make to really make this all come together.

Now, let's add another idea-this time from the Air Force heritage. In some ways, "info-warriors" are like Gen William ("Billy") Mitchell and the pioneer league of airmen. They see the potential. Mitchell's vision of the potential for airpower drove, at great cost to himself but great benefit to the nation, the development of a new form of warfare. Now here's the key point. Once the vision of strategic airpower was presented clearly, once people were able to say, "Yes, I see how this could change warfare," then the technologies followed: "Oh, air bombing-you'll need a bombsight." "Oh, enemy aircraft-we'll need some kind of detection system; let's call it radar." This is the point-the technology is not just a force

multiplier. It is the interaction of strategic vision with new technology that will produce the revolution in military affairs and a new warfare form.

This, then, is the challenge of information warfare. Is there something about information and the information technologies that would permit us to create such a mismatch between what, when, and how we and our opponents observe, orient, decide, and act or such a level of "information dominance" that the opponent is helpless-and not just on the battlefield? Is there a way we could use information, like current theories of airpower, to create an "information campaign" that engages an opponent simultaneously in time, space, and depth across the full range of his strategic structures so that the result is strategic paralysis (he is deaf, dumb, and blind to anything except that which we permit him to hear, say, or see)?[19] Not that we just blind him, but that he sees what we wish him to see without realizing that it's "our" reality, not his. Can we envision that kind of strategic information warfare? And, as was the case with airpower, technology will follow strategic vision. It's OK if we can't insert computer viruses by direct satellite broadcast-today; fry every air defense radar with an electromagnetic burst from a remote unmanned aerial vehicle (UAV)-today; transfer all the dictator's Swiss bank accounts to the internal revenue service (IRS)-today; project holographic images, complete with proper electronic signatures, of 15 squadrons coming in from the north when we're coming in the back door-today; or beam the Forrest Gump interview with "El Supremo" into every radio and television in banditland-today. Develop the strategic theory of information warfare, and the technology will come.

Information Warfare Doctrine

There is, of course, no official information warfare doctrine and the efforts of the various services to describe command and control warfare as the military application of information warfare remain incomplete. For the Air Force to focus almost exclusively on C2W that is defined as the "integration, coordination, deconfliction, and synchronization" of OPSEC, deception, PSYOP, electronic warfare, and physical destruction efforts targeted against the opponent's fielded military forces represents a failure to appreciate either air and space power or to appreciate how airpower doctrine could guide the development of an information warfare campaign. How, then, might we use current Air Force doctrine as presented in Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, as a template to start thinking about information warfare?

First, assume that information warfare is warfare in the information realm as is air warfare in the air and space realms. As the objective of air warfare is to control the air realm in order to exploit it while protecting friendly forces from enemy actions in the air realm, so the objective of information warfare is to control the "infosphere" in order to exploit it while protecting friendly forces from hostile actions taken via the information realm. Thus, as air control is usually described as counterair, with offensive and defensive counterair, so any strategy and doctrine of information control must address counterinformation in terms of offensive and defensive counterinformation. Offensive counterinformation, like offensive counterair, could be seen as involving information exploitation through psychological operations, deception, electronic warfare, or physical attack and information protection as, again, physical attack, electronic warfare (EW), and, often overlooked, public and civil affairs. Defensive counterinformation, like defensive counterair, would include active protection such as physical defense, OPSEC, communications security, computer security, counterintelligence, and, again, public affairs. Passive protection would include standard ideas like hardening sites and physical security.

like hardening sites and physical security.

If control, or dominance, of the information realm is the goal, like air control, it is not an end in itself but the condition to permit the exploitation of information dominance for, as in air doctrine, strategic attack, interdiction, or close "battlefield" support through C2W attack. Information dominance of both the strategic "battle off the battlefield" and the operational "information battlespace" is, like air and space control for traditional surface warfare, the key to strategic effect. The relevance of airpower doctrinal thinking for information warfare now becomes obvious. A review of the history of the airpower debates would show, in part, that those who insisted that airplanes were merely a force multiplier to provide close air support for the "real" effort would never recognize the strategic potential of airpower or support the acquisition of technologies for strategic air missions. As long as information warfare thinking is dominated by a doctrine that argues that the only information warfare mission relevant to the armed forces is command and control warfare and that C2W is merely a force multiplier against the communications and information assets of the fielded enemy forces, the potential for the exploitation of information dominance for strategic information warfare and, again, the identification and acquisition of key technologies will be missed. C2W, like close air support, is a vital military mission. It is, in fact, a central component of information warfare, but, like close air support and other "traditional" battle-oriented missions, not the whole story. The challenge is to use Air Force doctrine as the foundation to envision the "Information Campaign," which, like the "Air Campaign" in the Gulf War, is of strategic significance. What, for example, would "speed, precision, and lethality" be in an "info-strike?"

Epilogue: Danger of Not Developing Information Warfare Strategy

If the world really is moving into a third-wave, information-based era, failure to develop a strategy for both defensive and offensive information warfare could put the United States and the US military into the situation of being on the receiving end of an "Electronic Pearl Harbor."[20] Information is fluid; the advantages we now have, and which were demonstrated in the Gulf War, could be lost because we have very little control over the diffusion of information technology.[21] Second, it's a smaller world, and our potential opponents can observe our technologies and operational innovations and copy ours without them having to invent new ones for themselves.[22] Remember, the biggest center for developing new computer software is not Silicon Valley but Madras, India. What will they sell to whom? Finally, and to return to an earlier point, if the US military approaches information warfare merely as a force multiplier and adapts bits and pieces of technology to just do our current way of warfare a bit better-if we "digitize the battlefield" for an endless rerun of mechanized desert warfare-the real danger will be that someone else will refuse to play the game our way. What if they, like Count von Moltke or General Mitchell, think real hard, purchase the dual-use technologies on the free world market, alter their whole strategic concept, and make the leap to a strategy of information warfare?

We do not yet have a strategy of information warfare, and we have not answered the higher-order questions of how we would reorganize, retrain, and reequip for third-wave warfare. But if any of this has made even some sense, you now know the urgent requirement for developing the vision that produces the strategy. The strategy will identify the technologies, organizational changes, and new concepts of operations. We must really become like von Moltke and Billy Mitchell-"If we could use this to do that, then we could. . . ."

Notes

[1] Joint Chiefs of Staff, Memorandum of Policy 30, subject: Command and Control Warfare, 8 March 1993.

[2] Gen Gordan R. Sullivan and Col James M. Dubik, "War in the Information Age," *Military Review* 74 (April 1994): 46-62.

[3] Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers and Intelligence Systems* (Fairfax, Va.: AFCEA International Press, 1992).

[4]. Mary C. Fitzgerald, "Russian Views on Information Warfare," *Army* 44, no. 5 (May 1994): 57-59.

[5] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12 (April-June, 1993): 141-65.

[6] Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and State of the U.S. Air Force* , (New Brunswick, N.J.: Transaction Publishers, 1994).

[7] "Information Dominance Edges toward New Conflict Frontier," *Signal* 48 (August, 1994): 37-39.

[8] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994).

[9] Peter Black, "Soft Kill: Fighting Infrastructure Wars in the 21st Century," *Wired*, July-August 1993; 49-50.

[10]. Douglas V. Johnson, *The Impact of the Media on National Security Decision Making* (Carlisle Barracks, Pa.: Strategic Studies Institute, US Army War College, 1994).

[11]. John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22, no. 3 (Summer 1994): 24-30.

[12] H. D. Arnold et al., "Targeting Financial Systems as Centers of Gravity: `Low Intensity' to `No Intensity' Conflict," *Defense Analysis* 10 (August 1994): 181-208.

[13] John R. Boyd, "A Discourse on Winning and Losing," 1987. Unpublished set of briefing slides available at Air University Library, Maxwell AFB, Alabama.

[14] Maj George E. Orr, *Combat Operations C3I: Fundamentals and Interactions* (Maxwell AFB, Ala.: Air University Press, 1983); and Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: National Defense University Press, 1993).

[15]. Lt Col Norman B. Hutcherson, *Command and Control Warfare: Putting Another Tool in the War-fighter's Data Base* (Maxwell AFB, Ala.: Air University Press, September 1994).

[16] Newt Gingrich, "Information Warfare: Definition, Doctrine and Direction," address to the National Defense University, Washington, D.C., 3 May 1994.

[17] Joint Publication 3-13, "Joint Command and Control Warfare (C2W) Operations," second draft (Joint Chiefs of Staff, Washington, D.C., 15 January 1994).

[18] Gingrich address.

[19]. John A. Warden III, *The Air Campaign: Planning for Combat* (Washington, D.C.: National Defense University Press, 1988).

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

[21]. V.K. Nair, *War in the Gulf: Lessons for the Third World* (New Delhi, India: Lancer International, 1991), see especially chap. 4, "Role of Electronics in the Gulf War," and chap. 5, "Desert Storm: Air Power and Modern War."

[22] Jean Pichot-Duclos, "Toward a French `Economic Intelligence' Model," *Defense Nationale,* January 1994, 73-85 in *Federal Broadcast Information Service: West Europe,* 25 January 1994, 26-31.

Contributor

Dr George J. Stein (BA, Assumption College; MA, Pennsylvania State University, phD, Indiana University) is director, International Security Studies Core and professor of European Studies at the Air War College, Maxwell AFB, Alabama. Before joining Air University in 1991, Professor Stein had taught in the School of Interdisciplinary Studies, Miami University, since 1977. He was active in SPACECAST 2020 and continues his research in information warfare.

Disclaimer

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force or the Air University