Chapter Nine

# INFORMATION WARFARE: TIME FOR SOME CONSTRUCTIVE SKEPTICISM?*

*John Rothrock*

Future historians might well cite the years 1993 and 1994 as the period during which the U.S. 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. The concept is gaining momentum throughout the national security community at a breakneck pace.

Information Warfare's already strong institutional influence is readily evident in the spate of military and other national security organizations which have taken it on as a key element of their mission responsibilities or, as in a growing number of cases, which have been explicitly created to advance and pursue the concept. Simultaneously, millions of dollars are being programmed to provide new data bases, network architectures, advanced software, and other sophisticated capabilities all under the rubric of Information Warfare.

Also by now, most major military organizations have specially selected some of their best minds to help them define and address the new intellectual, organizational, programmatic, and technological challenges that the concept presents. Similarly, defense industry has

*This is a longer version of John Rothrock, "Information Warfare: Time for Some Constructive Skepticism?" *American Intelligence Journal*, Spring/Summer 1994, pp. 71–76. National Military Intelligence Association. Used by permission. A figure and all references to it were omitted for this version.

quickly and heavily come on board, seeing the concept to present a legitimate need and therefore also a business opportunity for bringing new, innovative mixes of its expertise to bear on post–Cold War problems. Throughout the national security community, belief in and enthusiasm for the concept seem to grow by the day as a key to coping with the ever accelerating changes that have continued to beset it since the fall of the Berlin Wall.

The following extended quote from the Secretary of Defense's 1994 report to the President and the Congress summarizes the compelling logic which undergirds this enthusiasm while also testifying to the broad acceptance which the concept seems to enjoy at the highest policy levels:

> Information Warfare is a means to not only better integrate C4I (Command, Control, Communications, Computers, and Intelligence), but also to address the comparative effectiveness of a potential adversary's C4I. It consists of the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and, in the process, achieving information advantage in the application of force. Thus, Information Warfare is an aggregation of and better integration of C4, C4 countermeasures, information systems security and security countermeasures, and intelligence.
>
> Information Warfare provides a method of better organizing and coordinating efforts to ensure an optimized information system responsive to the very demanding information requirements inherent in a smaller force structure, a rapid response capability, and advancing military technologies such as deep strike and precision guided weapons and enhanced mobility of forces. Information Warfare is an integrating strategy that makes better use of resources to provide for a better informed force—a force that can act more decisively increasing the likelihood of success while minimizing casualties and collateral effects.[1]

Certainly, if the first milestone for achieving a U.S. Information Warfare capacity suitable for the early decades of the coming century must be development of policy and resource support for the concept throughout the breadth and depth of the national security establishment, that objective now seems to be fairly well secured. The

concept's impressive thrust within the national security community has accelerated to the point where most briefings and discussions of the concept now acknowledge Information Warfare to constitute a new medium of conflict even beyond the military dimension to include new modes of global economic, political, and even cultural competition.

## ISSUES OF *THRUST* VERSUS *VECTOR* AND *MEANS* VERSUS *OBJECTIVES*

But, what *is* Information Warfare, beyond the nondiscriminating generalities of the DoD Annual Report and Claims that it is a new form of global competition for the Information age? The Information Warfare concept's policy and institutional *thrust* seems to be fairly well established. Now the challenge is to address the intellectually even more difficult issues of its vector.

Thus far, the specifics of the concept's achieved thrust have focused primarily upon organization, process, and resource issues—i.e., essentially the means of Information Warfare. But, beyond the generalities of the DoD Annual Report and claims of the concept's relevance as a new ubiquitous form of Information Age competition and now well established military objectives of countering enemy command and control while protecting your own, the *objectives* of Information Warfare remain relatively undefined. And, with the concept's objectives undefined, its potential implications also suffer from underdefinition and, therefore, lack of examination.

Much of this tendency to shy away from difficult definitions of conceptual objectives has to do with the traditional American intellectual style which is one of pronounced pragmatism. The American institutions generally—and the American military particularly—are decidedly more comfortable with process than with theory, with action more than reflection, with efficiencies more than effectiveness (there is often a difference), with particular performance than with general coherence, and with the particular more than with the holistic.

This inclines the U.S. military, along with many other American institutions, to reduce general propositions such as Information Warfare as quickly as possible to specific "means" issues—i.e., essentially

those of resources, organization, and process—with relatively less attention paid to the more general concerns associated with objectives and the more integrated, more coherent address that such concerns demand. Traditional American resource management tools—including the DoD Planning, Programming, and Budgeting System reflect and reinforce these tendencies.

While this especially American style proves its practical mettle over and over in dealing effectively with specific problems, it has definite weaknesses in its capacity to treat several problems at once in context with each other. Unfortunately, it is exactly this sort of integrated, contextual address that an idea as complex and far-reaching as Information Warfare demands. Today, it is far from certain that the structure of institutional relationships and processes through which the U.S. Government manages the country's global security affairs—the PPBS, service department and joint service doctrinal and organizational relationships, the functional junctures of military and civil infrastructures, to name just a few—can cope with Information Warfare in all of the dimensions and manifestations that the concept's logic demands.

## SOME CHALLENGING QUESTIONS

Today, when one reads about Information Warfare and hears about the concept in presentations, it remains very difficult to determine if there is anything that Information Warfare is not. A skeptical mind is soon prompted to ask, "*If Information Warfare is everything, can it be anything?*"

Several other questions might follow. For example: Is, as some of its harsher critics suspect, the concept primarily of a bureaucratic and resources thrust toward specific means with little intellectual vector toward specific objectives? Is it truly a trend or merely "trend surfing"? Might not the concept be fundamentally flawed intellectually in constituting, as it does, an attempt to *explicitly* address phenomena (those of information) which are *implicit* to all human endeavor, including warfighting? Is there a risk that Information Warfare could become a convenient lip-service repository for all of the difficult issues of post–Cold War relevance for a national security structure and military whose general forms and culture remain rooted in Cold War

precepts? ("Sure, we're relevant in the new era, we subscribe to Information Warfare.")

And, more specifically: If Information Warfare holds that all or most information is valuable and targetable but that it also must be accessible and readily "fungible," what are the implications for traditional concepts of information security and classification? Can classified, heavily compartmented approaches—running as they do essentially against the grain of the Information Age's defining characteristic, that of information proliferation—be effective in pursuing a military concept supposedly suited specifically to the character of that age? Where do the military's purview and responsibilities concerning Information Warfare and information security begin? Where do they end? Are the American society and its military, as the most information-dependent society and military in the world, really wise in advocating Information Warfare as our preferred new style of conflict? If, as is increasingly espoused, Information Warfare is more than just a military proposition, must the society as a whole be capable of pursuing—and defending against—it if the military is to be able to do its part effectively? If the society has problems in meeting IW's challenges (say, for example, in mustering the national will that the concept's defensive imperatives presume), does the military have an appropriate role in helping the society deal with such non-military requirements and implications? If so, what is that role?

These are hard but fair questions which the quickly forming Information Warfare community should be prepared to answer. At a minimum, their serious consideration should provide the concept with an intellectual vector appropriate to its thrust—of course, that is *if* Information Warfare is more than the mere fashion that some skeptics suspect it to be and, also, if our national security structure is capable of recasting itself adequately to effectively implement such a comprehensive idea. If the concept is faultable on either of the latter points, the questions would of course ferret that out as well.

## A SUGGESTED PRISM THROUGH WHICH TO CONSIDER INFORMATION WARFARE

But, how are such questions most effectively addressed? Is there perhaps a particularly suitable intellectual prism through which to

consider Information Warfare with the necessary rigor appropriate to the importance that the concept's advocates claim for it? How best to explicitly examine a spectrum of issues as implicit to so many other considerations as those comprising Information Warfare?

## THE "INFORMATION WARFARE ARROW"

The head of the "Information Warfare Arrow" is comprised of intellectual effectiveness of a highly complex sort. Probably more so than any other form of global security competition, Information Warfare will require exceptional intellectual mastery of the important but subtle hierarchical relationships between policy, strategy, operations ("campaigns"), and tactics. It will equally demand a sophisticated appreciation of the relationships of all of these perspectives to technology. Without such mastery of these relationships, Information Warfare carries with it great risks.

The best technology, even when employed with the greatest of tactical effectiveness, can be counterproductive if the technology and its employment are not orchestrated against a set of well conceived, hierarchically consistent operational, strategic, and policy objectives. While this observation is true regarding any military or quasi-military undertaking, it is especially important regarding Information Warfare which is first and foremost an intellectual rather than a technological or physical undertaking. Information Warfare carries with it especially heavy risks of "winning battles but losing wars." The best of technology and tactics cannot protect against these risks in the face of poor policy, strategy, and operational concepts and the unprecedented degree of conceptual, doctrinal, structural, procedural, and technology integration—i.e., *far beyond "jointness"*—that effective Information Warfare is certain to demand.

The arcane (and now largely irrelevant) policy and strategic machinations of the Cold War excepted, Post–World War II U.S. military thinking has been generally at its best at the levels of tactics (i.e., the specifics of "employment") and technology. True, the 1970s saw a renewed appreciation of the "operational art" perspective (also known as the "campaign level") of military employment and the Gulf War demonstrated that since then we have made great strides in organizing ourselves at that level. However, most observers agree that the operational level still does not yet constitute our military's long

suit. Yet, excellence at the operational level is vital to success in Information Warfare for it is the conceptual bridge between higher-level objectives and the means for achieving them.

Beyond these concerns, our system of government necessarily places considerable ethical and political burdens upon those charged with developing policy, strategic, and higher-level operational *objectives*—burdens that are rooted in a logic borne of tradition and culture that goes far beyond the exigencies of any particular set of global security considerations. The net result is a national security and military structure that is much more comfortable in addressing the technological and resource *means* of conflict than it is in considering the higher policy and strategic objectives of conflict.

For this much greater proficiency regarding means as opposed to objectives not to constitute a potentially fatal flaw in the United States' pursuit of Information Warfare—certainly if the concept is carried to its ultimate logic—will require fundamental changes in how we understand conflict and the appropriate responses of our society to it. In fact, the changes that might be required could be so great as to raise a legitimate issue of not only whether we can but even of whether we should make them, the challenges of Information Warfare notwithstanding. Does our society *want* to be the sort that is adept at the degree and types of control of information that some of the more enthusiastic advocates of Information Warfare seem to presume?

This brings us to the concept of national will. Advocates of Information Warfare must discipline themselves to assure that the overall concept—or any particular aspects of it, even those under cover of heavy security classification—do not conflict with or exceed the imperatives of the national will and the crucial *bond of trust* between people and their government. The loss of this trust would obviously be the greatest Information Warfare disaster that can be imagined.

An Information Warfare concept that depends upon an unrealistic or warped perception of the national will, while possibly still maintaining its means thrust will certainly lack appropriate vector, possibly even to the point of coming back to victimize those employing it. In judging how and to what degree specifics of Information Warfare employment are or are not commensurate with national will, it will

always be instructive to look at the factors of culture, politics, economics, and infrastructure (all as perceived by the society). If a concept runs against the reality or the societal perception of any of these guiding factors, it must be regarded as highly risky. Again, reliance upon heavy security classification to protect a concept from the extent to which it might run against the societal grain can only exacerbate the possibility and potential consequences of its failure.

## INFORMATION WARFARE EMPLOYMENT AND DOCTRINE

Even if fairly conservatively applied, the Information Warfare concept will require highly integrated, *holistic* employment throughout the policy > tactics/technology spectrum of perspectives which must exceed anything our current military culture and structure has ever demonstrated to date. (If, as is implied in the narrower articulations of the concept, Information Warfare remains confined to the tactical level and middle/lower rungs of the operational perspective—such as during the Gulf War—one might ask what is to differentiate "Information Warfare" from what are now more or less conventionally held "Counter Command and Control" concepts.[2]) Without this high degree of integration, the concept is certain to founder in its practical employment for lack of coherence.

As in all military associated employment, the key to coherence in Information Warfare will be effective doctrine. In addition to the several perspectives portrayed by the "arrow," this doctrine—and the structures and procedures it implies—will have to acknowledge Information Warfare to include *three highly interdependent spheres of competition* with actual and/or potential adversaries of the United States. These are (1) the *capacity for offensive action* against the enemy's decision-making structure and processes; (2) *protection of our own capabilities* to make and effect decisions; and (3) the *capacity to create and use information for our own purposes* more effectively than adversaries can create and use information for their purposes.

Underlying all of these relationships, and adding to their maddeningly subtle complexities is a curious but unavoidable irony that is implicit to the Information Warfare concept: i.e., that the U.S. must develop very sophisticated and complex means for attacking adversaries' typically far less developed information/decision structures

while still further having to protect our own highly developed infrastructure from relatively simple—but potentially grievous—threats.

## The Offensive Sphere

Of the three competitive spheres, the heavy preponderance of attention currently given Information Warfare seems certainly to focus on the concept's *offensive* potentials. Not only does this reflect the U.S. military's natural offensive affinity, it also probably reflects the fact that offensive concepts are less fettered by limitations of established U.S. information practice, structure, and process. An already observable feature of this is the tendency for Information Warfare responsibilities—even seemingly operational ones—to migrate into organizations that are part of—or which are at least heavily involved with the Intelligence Community (especially its SIGINT Components). These are organizations that, at least in theory, are most suited to assessing targets for Information Warfare applications.

How these Intelligence-focused organizations will handle the inherent tension between the natural intelligence inclination to exploit enemy information for its intelligence potential and the operators' natural inclination to destroy or disrupt enemy information sources and flows is certain to become a major doctrinal issue. (A cynic might see something here akin to the Intelligence fox being put in charge of the Information Warfare henhouse.) Whoever is responsible, the necessary doctrinal responsibility and authority to assure that offensive applications accord with all levels of conflict perspective—tactical up through the policy level—are sure to be demanding ones and to require concepts of organization and process for which there is little precedent.

## The Protective Sphere

The *protective* (i.e., "defensive") aspects of the Information Warfare concept are even more difficult to handle doctrinally, structurally, and procedurally. This is because convenience and operational efficacy in the handling of information usually imply vulnerabilities in the information and decision-making processes which can be fairly readily assessed and exploited/interfered with by an adversary.

Strong doctrinal guidance will be required to direct the IW concept through the maze of "either-or" issues that this tension between general security and immediate efficacy must inevitably raise. Whether a community which is heavily imbued with an Intelligence perspective can adequately define, let alone resolve such issues remains an important question.

## The Competitive-Use-of-Information Sphere

As complex as these first two competitive spheres of the Information Warfare concept are, they pale in difficulty in comparison to the third—that of the relative effectiveness of our own information handling and decision-making structures and processes.[3] This is where subtle asymmetries between our own objectives, capabilities, and information dependencies and those of adversaries, if not readily recognized and taken into account, can wreak disaster.

It might be useful to characterize the situation as follows: We must always be prepared to see ourselves as highly sophisticated "cyber-warriors" who might eventually need to be able to attack and defend against enemies much of our own kind. But we need more immediately the capacity to attack and defend against the equivalent of clever Information Age "neanderthals" who are less dependent upon sophisticated information means than are we but who have adequate sophistication to understand and means to exploit that fact.

Even without considering direct attacks against each other's information/decision capacities notwithstanding, the effective use of information to make timely appropriate decisions is a highly complex proposition. Again, it is a challenge primarily of intellect and only secondarily is it one of technology.

Viewed in this sense, the Command and Control process must be seen as one too profound to be left to those who are merely expert in its technical means—i.e., "communicators," computer specialists, experts in the technologies of information, and the like who in our military culture are most closely identified with the means and processes of Command and Control. To relegate the C2 information/decision-making process to the technical perspectives of these specialists would be uncomfortably analogous to having the telephone company install a telephone for you then expecting them to

tell you what to say on it. The best of C2 technology and technology architectures cannot substitute for the conceptual and intellectual quality of the decisions they support.

To achieve the sophistication and doctrinal coherence and effectiveness necessary to provide that quality, especially in response to the unprecedented demands of Information Warfare, will the U.S. military culture to accept at least two conceptual distinctions with which it naturally has trouble.

First, the military must be able to better distinguish between "*efficiency*" *and* "*effectiveness*" in order to be sure that, in regard to a specific situation or objective, it is not "doing the wrong thing well." Especially in terms of Information Warfare effectiveness, the need to make such distinctions requires great effort in developing new—essentially non-attritively based measures of merit—by which to gauge the meanings of effectiveness which the concept implies.

Second, Information Warfare requires sophisticated distinctions to be made between hierarchical levels of the cognitive process by which data and information contribute to effective decisions, a process which Information Warfare wants to degrade for the enemy and to preserve and enhance for ourselves. Chief among these distinctions are those between "*awareness*" (the lowest level of cognition), "*knowledge*," and "*understanding.*" One can be "aware" of something but not know its specifics. Similarly, one can "know" something, even very well, but not "understand" its full implications, especially as they impact and are impacted by specific circumstances. (For example, the West "knew" a lot about the Soviet Union, but, as it turned out, our "knowledge" far exceeded what we actually "understood" about it.)

The two principal objectives in Information Warfare must be (1) to degrade adversaries' capacity for *understanding* their own circumstances, our circumstances, and the circumstances that affect all sides while preserving and enhancing our capacity for such understanding and (2) to degrade adversaries' capacities to make *effective use* of *whatever correct understandings* they might achieve and, again, to preserve and enhance our own capacities in this regard. (Note: As in earlier history, future conflicts could well be multilateral, with alliances brief, partial, and calculated often only for the

most fleeting advantage; this is yet a further practical complication which Information Warfare advocates must directly confront.)

Achieving and preserving the advantages that will accrue in winning such a competition will be fundamental to future success in the future global security competition that is likely to evolve. As such, Information Warfare cannot be pursued as something "exotic" and separate from the mainstream of the command, control, and employment of military forces. Therefore, the ultimate Information Warfare question is this: Is the U.S. national security structure capable of the intellectual and doctrinal suppleness required to pursue an implicit set of concerns and issues using highly calculated, *specific* means, to achieve *explicit*, but *coherent* objectives?

Yet again, whether or not the limitations of our previous military experience and the resulting U.S. national security/military culture and intellectual style that it has produced will permit us to effectively meet the doctrinal demands for conceptual and employment coherence which Information Warfare poses must at this point remain an open issue.

## CONCLUSION

Obviously, the post–Cold War era, most notably the aspects of it that comprise the "Information Age," requires a new approach to global security. "Information Warfare" is gaining considerable momentum as the conceptual vehicle with which the United States, especially the military, hopes to meet this challenge. However, the concept's far-reaching and complex implications dictate degrees of intellectual, structural, and procedural coherence that would exceed by far anything that the modern U.S. national security/military structures have achieved in the past.

For this reason, an objective observer must remain skeptical—if also hopeful—about Information Warfare's historical viability as a new global security concept for the United States. It seems that the only thing more difficult than readying ourselves for Information Warfare would be to conceive of an alternative to it.

## NOTES

[1]Les Aspin, Secretary of Defense, *Annual Report to the President and the Congress*, Washington, D.C., January 1994, pp. 227–228.

[2]This is not to imply that we have now finally adequately developed our Counter Command and Control concepts and capabilities, even at the tactical and lower operational levels. To appreciate the full complexity and potential/implications of information conflict on those and also higher planes, see especially V.V. Druzhinin and D.s. Kontorov, "Concept, Algorithm, and Decision," Moscow, *Voinizdat*, 1972. (One of the USAF "Soviet Military Thought" translation series.) Counter C2 and information Warfare concepts that are not rooted in appreciation of issues raised by Druzhinin and Kontorov probably should be held intellectually suspect. (However, it is not necessary to agree with the authors' decidedly Soviet conclusions about many specific issues.) For a more recent, perhaps even deeper discussion of information and its use/manipulation, see also Keith Devlin, *Logic and Information*, Cambridge (UK), Cambridge University Press, 1991. For a less theoretical treatment applicable to the tactical and operational levels, see as well the current author's "Counter Command and Control in Conceptual Perspective," *Air University Review*, Jan–Feb 1980. This article, while dated in its focus on the Soviet adversary, explores several conceptual issues which probably still warrant consideration.

[3]It is in recognition of the complexities that this section addresses that the National Defense University has designated the curriculum it intends to address these issues as a curriculum in "Information-based Warfare." Others are also coming more frequently to use this term to capture the full complexity of the concept.