P7

INFORMATION WAR - CYBERWAR - NETWAR

Prof. George J. Stein

Air University
Air War College
325 Chennault Circle
Maxwell AFB AL 36112

(205) 953-2127
(DSN) 493-2127

INFORMATION WAR - CYBERWAR - NETWAR

Strategy, according to the Department of Defense, is the "art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat." For most people it is obvious that the *political* and *economic* aspects of the *national* security policies of the United States are developed by the national political authorities, the President and the Congress, and, in dealing with foreign states or groups, executed by the Departments of State, Commerce, Agriculture, or whatever. Policies for the development and use of *military* forces are, likewise, formulated by the national political authorities and conveyed to the armed forces through the Secretary of Defense. Few people, however, have paid much attention to just how *psychological* forces are to be developed to support national policies and, more importantly, by whom these *psychological* forces are to be developed and, most importantly, by whom will these forces be used, with what authority, and to what ends. The development of new tools and technologies for communication, especially those based on computers and other aspects of the information highway, have brought the potential for *psychological warfare*, that is, "Information Warfare," from the realm of science-fiction to deployed reality.

The futurists Alvin and Heidi Toffler have argued that the United States armed forces need to develop a "systematic, capstone concept of military *knowledge strategy*" which would include clear doctrine and policy for how the armed forces will acquire, process, distribute, and project knowledge and information to serve national strategy.[1] Quoting from the "Memorandum of Policy No.30" (6 May 93) of the US Joint Chiefs of Staff, the Tofflers argue that the concept of Information War has been expanded to include psychological operations aimed at influencing the "emotions, motives, objective reasoning, and ultimately the behavior" of others.[2] Such an evolution of traditional warfare in the direction of Information War is the logical result of the transformation of the chief forms of American society's mode of wealth generation from land, through natural resources and industrial infrastructure, to knowledge/data/information as the new creators of wealth. "First Wave" wars fought over land; "second wave" wars fought over physical productive capacity; the emerging "third wave" wars will be for the access to and control of "knowledge." As the "combat form" in any society follows the "wealth-creation form" of that society, the wars of the future will be predominately, but not solely, "Information Wars."

While there are not yet any official or agreed definitions, "Netwar" and "Cyberwar" are emerging as key concepts in any discussion of Information War. Originally the concepts seem to have been invented by the science fiction community as, for example, in the very throught-provoking operational environment of future war suggested in Bruce Sterling's *Islands in the Net*.[3] More recently, the concepts of netwar and cyberwar have been developed in the important exploration by J. Arquilla and D. Ronfeldt, "Cyberwar is Coming!"[4] Their suggestions provide a thoughtful starting point for exploring the military and civil/military issues of Information War.

Netwar is seen as "societal-level ideational conflict waged in part through internetted modes of communication."[5] That is, netwar is *strategic* level conflict, it is about *ideas and epistemology*, and it is waged largely, but not entirely, through a society's communication nets. The target is the human mind. Thus, one could argue that certain aspects of the Cold War had the characteristics of a dress-rehearsal for future netwar: Radio Free Europe, the Cominform, the US. Information Agency, *etc.* While the concept of netwar in its communications net context appears to be most relevant to traditional state-to-state conflict through the use of a nation's electronic intelligence assets, the proliferation of non-state political actors such as Greenpeace, Amnesty International, or ideological/religious inspired movements with easy access to world-wide computer networks for the exchange of information or the coordination of political pressure on a global basis, suggests that the "government" of a "nation-state" may not be the "center of gravity" against which "war" is waged.[6] Netwar between and among non-state actors is not too difficult to imagine.

At first glance, netwar may appear to be a technogeek word for good, old-fashioned propaganda. It would be comforting to believe that the technology to manipulate propaganda has just improved a bit and the same "tried and true" methods still worked. The recent Gulf War showed both Sadaam Hussein and the Alliance still in the "old school."[7] There were the classic "atrocity" accusations of (1) bombed baby-milk factories and (2) stolen baby incubators from Kuwaiti hospitals; the classic inflation of the stakes of the conflict with the (1) future of the new world order and (2) the mother of battles for the future of Islam in the balance; the classic "us or them" polarization in which "neutrality" or unenthusiastic support {*e.g.* Japan} was decried; and the classic "God is with us" by both sides. And, while there was a bit of standard "demonization" of the other side with Saddam as the new Hitler and President Bush as the "Great Satan," the Gulf War was unusual in that there was far less demonization or dehumanization of the opponent.

Perhaps the multicultural nature of the Alliance precluded turning the Iraqi army into something subhuman. Indeed, there may have been a spark of netwar genius in treating the Iraqi soldiers as "brave men put into an impossible situation by a stupid leader." No dishonor in surrendering then. And, there may have been a glimpse of the future when, thanks to the technologies available for cyberwar, Baghdad Radio signed on one morning with "The Star-Spangled Banner."

Traditional propaganda, however, was usually targeted via mass media to influence a mass audience. One key change consequent of contemporary technologies is the potential for the "demassification" of propaganda. Anyone who has received individually targeted advertising from a company specializing in "niche" marketing research must have had a momentary shudder when they realized that there are private companies "out there" who seem to know everything about our buying habits and tastes. Contemporary data bases and the constantly expanding multiplicity of sources, media, and channels for the transmission of information have created the opportunity, and "target sets," for custom-tailored netwar attacks. Computer bulletin boards, cellular telephones, video-cameras tied to fax machines -- all provide an entry point and dissemination net for customized assault by governmental, commercial, and private interests.

A major new factor in Information War results directly from the world-wide internet of broadcast news. Some people have begun to realize that governmental decisions could become increasingly "reactive" to a "fictive" universe created by CNN and its inevitable competitors. The media-created universe is "fictive" rather than "fictional" because what is shown may be "true;" it is just not the whole, relevant, or contextual truth. Nevertheless, this "fictive" universe becomes the politically relevant universe in a society in which the government is supposed to "do something."[8] Somalia gets in the news and the United States gets into Somalia despite the reality of equally disastrous starvation, disorder,

and rapine right next door in Sudan. No reporters with "skylink" in Sudan. The potential for governments and non-state interests to manipulate the multi-media, multi-source fictive universe to "wage societal-level ideational conflicts" should be obvious.

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 actors through increasingly de-massified networks. The niche-propaganda potential available to states with access to the universe of internetted communications via, for example, the networks over which business, commercial, or banking information is transmitted to suggest that a "hostile" state is about to, say, impose price controls, could easily provoke financial chaos. The target state would not know what had happened until too late. Direct satellite broadcast to selected cable systems, 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 their clansmen from the army. In essence, niche-info in an increasingly multi-source fictive universe offers new possibilities.

If the new capabilities of already publicly known technologies to "simulate" reality are added to the arsenal of netwar, a genuinely revolutionary transformation of "meta-propaganda" becomes possible.[9] That is, traditional meta-propaganda attempted to discredit the other side's propaganda by showing, for example, that "official" casualty figures were demonstrably false and, consequently, all "news" from the government was equally false. The credibility of the opponent was the target and the strategic intention was to separate the government from the people. That is, standard Clausewitzian trinitarian warfare {population, government, armed forces} via radio and leaflet. Today, however, the mastery of 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 which exists in "effects" though not in fact. Stored video images can be recombined endlessly to produce any effect chosen. Now, perhaps, "pictures" will be worth a thousand tanks. Of course, "truth will out" eventually and that may be true. Some day, someone will discover that the nationwide broadcast by the maximum leader calling on all loyal citizens to return to their homes and fields and cease fighting was created in Hollywood, through out-sourcing, and broadcast by the commercial "NETSTAR-IV" system completely unbeknownst to their own engineers. Netwar is beginning to enter the zone of illusion.

This needs a bit more attention. Through hitching a ride on an unsuspecting commercial satellite, a "fictive simulation" is broadcast. This is not science fiction. Simultaneously, various "info-niches" in the target state are accessed via "the net." That sentence has a lot of implications, both technical and political. In any event, some of these targets receive reinforcement for the fictive simulation; other receive the "real" truth; others receive merely slight variations of the target state's anticipated responses. What is happening here?

This is not traditional meta-propaganda in which the target is discredited as a source of reliable information.[10] Rather, the very possibility of "truth" is being replaced with "virtual reality;" that is, "reality" which produces effects independent of its reality. What is being attacked in a *strategic* level netwar is not only the emotions, or motives, or beliefs of the target population, whether mass or niche, but the very power of objective reasoning. The fictive simulation of the maximum leader's call to stop fighting would, of course, be followed immediately by a "real" broadcast in which the maximum leader exposes the netwar attack as propaganda invented by "culture destroyers in Hollywood." Parts of the society have received, via the demassified info-niche attack, evidence that the maximum leader is telling the truth, others that he is lying, still others increase their confusion when

the legitimate state "Voice and Vision" broadcasts warnings against the cunning of the enemy. In a society under assault across the entire infosphere, there is no way for members of that society to verify internally the truth or accuracy of anything. Objective reasoning collapses.

At the *strategic* level, the ability of "observe" is flooded by contradictory information and data; more importantly, the ability to "orient" is vitiated by the elimination of the possibility of objective reasoning; "decisions" respond to a fictive or virtual universe and; of course, "actions" become chaotic as there is no "rational" relationship of means to ends. It would seem, then, that *strategic* level netwar or Information War brings us within sight of that elusive "acme of skill" wherein the enemy is subdued without killing. The reality of communication may, however, be more complex than the Info-warriors imagine. "Societal-level ideational conflict" may need to be considered with all the care given to the conduct of nuclear war as the "end state" of netwar may not be bloodless surrender, but total destruction of the targeted society.

Any discussion of Information Warfare, netwar, cyberwar, or even perception manipulation as a component of command and control warfare by the armed forces of the United States at the *strategic* level must occur in the context of the moral nature of communication in a pluralistic, secular democratic society. That is, the question must be raised whether the use of the techniques of information warfare at the strategic level is compatible with contemporary American purposes and principles. Likewise, the question must be raised whether the armed forces of the United States have either the moral or legal authority and, equally important, the practical ability to deploy the techniques of Information Warfare at the *strategic* level in a prudent and practical manner. There is reason to be skeptical.

According to the philosopher Eric Voegelin, the moral basis of communication in any society can be discussed in terms of its substantive, pragmatic, and intoxicant functions.[11] The *substantive* purpose of communication is the building or developing of the individual human personality; it is simultaneously the process by which a substantive, real-world community of "like-minded" persons is created, developed and sustained. At the most trivial level, the moral purpose of substantive communication can be illustrated by contemporary American efforts to remove sexist or racist language from accepted use as these forms of communication are perceived as an affront to the individual dignity of fellow citizens and as destroying the self esteem of a part of the community. At a more serious level, the debates in American society about prayer in the public schools illustrate the substantive and formative nature of communication in society, as "private religious views" must not corrupt the public formation of character for life in "modern" America. Finally, any real world society rests on the substantive communication and understanding among its members. Society is no mere "external" structure of relationships; it is a universe of "meaning," a "cosmion" according to Voegelin, "illuminated with meaning from within by the human beings who continuously create and bear it as the mode and condition of their self-realization."[12]

The attempt by several nations such as China, Iran, or Saudi Arabia to "insulate" their societies from the effects of the global communications network illustrates their awareness that the continued existence of their societies may depend on a shared substantive universe of discourse unique to their societies. Even within the West, the self-consciousness of the French that the continued existence of France as a distinctive society organized for action in history may require state intervention in the substantive content of communication within society through limiting the percentage of "foreign" broadcast material illustrates the seriousness with which the substantive nature of communication is taken by other nations.

The recognition of the substantive function of communication is, however, problematic in American society as the dominant ethos of much of the political class has reduced "morality" or character formation to a question of private prejudice. The person who, for example, would argue that homosexual actions represent immoral or deviant behavior need not be considered seriously. Religious arguments that abortion is wrong as it violates "natural law" are marginalized politically as "private opinion." How long the armed forces will continue to be permitted to discipline an officer on the basis of such a quaint concept as adultery remains to be seen.

The *pragmatic* function of communication in society is reasonably straightforward. That is, pragmatic communication consists of the techniques for influencing other persons to behave in ways the communicator wishes. Only behavior matters. Most political and commercial communication is merely pragmatic. It is usually indifferent to the substantive moral content of the communication and usually functions autonomously to mold perception, and consequently behavior, to the purposes of the communicator. The target of pragmatic communication becomes an object for manipulation. The morally dubious quality of an advertising industry devoted to the development of the personhood of Americans as consumers of superfluous material goods needs little comment. The morally dubious quality of political advertising which seeks to reduce civic discourse to conditioned response to sound-bytes and slogans, again, needs little comment. The pragmatic use of communication in an Information War or attempt at perception manipulation by the armed forces is, of course, the real issue.

Finally, the *intoxicant* function of communication in American society needs little comment. The addiction of considerable segments of the citizenry to talk shows, soap operas, romance "novels," professional sports broadcasts, and other well-known forms of

distraction and diversion are well catered to by the "entertainment" industry. Whatever the morality of the entertainment "pushers," the intoxicant quality of much contemporary communication is more a commentary on the bored, empty and confused personalities of the addicts.

For Voegelin then, civil communication in contemporary American society would be described as being dominated almost entirely by the intoxicant and pragmatic modes. More importantly, the absence or deformation of substantive communication in public life is defended by the secular and liberal political class in the name of freedom, pluralism and multiculturalism. Pluralistic America is a society in which "the formation of opinion is left, through the use of various means of communication, to private initiative, as distinguished from a 'unitary' society, in which mass opinions are formed through various types of governmental action."[13]

Netwar or strategic level Information War attacks another society's decision-making process. Likewise, cyberwar or *operational* level Information War attacks the decision-making process of the enemy armed forces. At the operational level of war, a national Information War or netwar strategy is translated by the armed forces into cyberwar or "command and control warfare," often referred to as "C2W." Cyberwar, in the hands of the local Joint Force Commander, attacks the "mind" of the enemy commander though various tools, some of which are from the universe of electronic warfare, to produce "bad" decisions and prevent, delay, or deny information for "good" or operationally effective decisions. The goal of Information War at the *operational* level is to deprive the enemy commander control of his battlefield assets while, of course, preserving friendly command and control capabilities. Again, the goal is to deprive the enemy commander *control* of his assets; this may or may not involve physical destruction. Successfully applied, operational level information war or cyberwar influences the emotions, motives, objective reasoning,

and ultimately the behavior of the enemy to separate the enemy forces from the enemy leadership. It is in many ways similar to the "decapitation" strategies of nuclear war.

Cyberwar or C2W may represent the strategic form required by the explosion in communication and information technologies but it should not be confused with more "traditional" forms of combat support through electronic warfare. Cyberwar or C2W is not merely attacking the enemy's command and control systems, especially his infosphere, with high-tech precision munitions or electronic jamming while protecting one's own systems. That has always been part of modern warfare. Electronic warfare is merely one part of cyberwar. Electronic warfare normally involves electronic support to identify, locate or intercept enemy electromagnetic emissions, electronic protection of friendly forces and equipment from hostile electronic warfare, and electronic attack by electromagnetic or directed energy means of enemy forces and equipment to degrade, neutralize or destroy enemy combat capabilities. In addition to electronic warfare, cyberwar or C2W includes operational security, deception, psychological operations, and, of course, physical destruction. Cyberwar, then, in not merely fancy electronic battlefield preparation for traditional maneuver or attrition battles. More importantly, destruction, actually putting iron on the target, is only one aspect of cyberwar and, ideally, may not be necessary if the Joint Force Commander has successfully employed the four other "tools" of cyberwar: electronic warfare, deception, psychological operations, and operational security.

Operational security is a fairly simple concept but, in the context of Information War, may be very difficult to accomplish. In essence, the commander must identify what information is critical to an enemy, what information an enemy might be able to access, analyze his own actions which might reveal information and, equally vital, develop the full range of infosphere security against threats of monitoring, hackers, hostile penetration, and virus contamination. Deception and psychological operations, again fairly traditional

military concepts, may be combined with operational security to provide a full array of assaults on the enemy's ability to form or sustain the accurate situational awareness required for successful command and control of his own forces. Deception can range from classic efforts such as the 8th Air Force bombing of Pas de Calais to draw the Germans away from Normandy to more contemporary efforts such as the Marine Expeditionary Force lurking off the coast near Kuwait city during the Gulf War. Electronic deception can involve the generation and broadcast of message traffic between totally non-existent units or false messages from actual units. Psychological operations, again, are well understood but, in the context of the quantum leap in transmission and distribution capabilities, such operations will increase in intensity and importance. The well-known ability of aircraft like *Commando Solo*, an EC-130 deployed during the occupation of Panama, to over-ride the local radio and television networks with "friendly" broadcasts merely hints at what, logically, will "proliferate" to other nations and "migrate" to space-based systems.

Cyberwar or C2W strategy , as Arquilla and Ronfeldt observe, may change not only the nature and location of the battlefield from terrain to space and the infosphere, but change the very idea of "victory" or "defeat." Replacing classical attrition war with maneuver war through increased speed and lethality, as in the Gulf War, may be simply attrition "put on wheels." Cyberwar, on the other hand, *may* permit campaigns without bloody battles; wars "won" by "striking at the strategic heart of an opponent's cyber structures, his systems of knowledge, information, and communications;"[14] that is, "victory" without the need to destroy the enemy's armed forces and, to return to *strategic* level netwar or Information War, without the need for the enemy to even know there has been a conflict. It may not, however, be that simple.

Strategy, recall, is the "art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat." Strategy is the means to achieve an end, with military strategy serving a political or policy purpose. Sound military strategy requires influencing the adversary decision-maker in some way that is not only advantageous, but reasonably predictable. A national security strategy of Information War or netwar at the *strategic* level, that is, "societal-level ideational conflict waged in part through internetted modes of communication," and an *operational*-level cyberwar or C2W campaign to decapitate the enemy's command structure from its body of troops, may be "advantageous" but, more importantly, may *not* produce effects that are reasonably predictable. Conflict is about a determinate *some* thing, not an indeterminate *any* thing. The goal of influencing the adversary's ability to "observe" by flooding him with contradictory information and data; vitiating his ability to "orient" by the elimination of the possibility of objective reasoning; and forcing "decisions" to respond to a fictive or virtual universe will, of course, produce "actions," but they will be actions which are chaotic, random, stochastic and inherently *unpredictable* as there is no "rational" relationship of means to ends.

In the context of *operational*-level cyberwar or C2W, this may be an acceptable military strategy. The inherently unpredictable and stochastic nature of combat, Clausewitz's "fog and friction," is amplified by successful cyberwar. A successful cyber-strategy depends on the ability of the Joint Force Commander to deploy his power assets, especially combat forces, *not* to dominate the enemy decision-cycle {which, after all, has just been rendered chaotic}, but to exploit *opportunities* as they evolve stochastically from the disoriented, decapitated or irrational enemy actions.[15] The "fast transient maneuvers" beloved by fighter pilots are less about speed and more about maneuver.[16] Cyber-strategy

is the control of the evolution of the power distribution to impose the Joint Force Commander's "order" on the enemy's "chaos." As Sun-Tzu observed, "those who are able to adapt to changes in the enemy and achieve victory are considered supreme."[17] The threat exists, however, that the destruction of enemy rationality may collapse "battle" into mere "fighting" with no outcome but surrender or death. Sun-Tzu also observed that "when battles gain victories and attacks achieve occupations, yet these successes are not followed up, it is disastrous. This is known as 'persisting turmoil'."[18] Operational-level cyberwar may, then, be the very "acme of skill" which reduces the enemy will without killing; it may also be the very abolition of strategy as it attacks the very rationality required for war termination.

The tools, techniques and strategy for cyberwar or C2W will be developed and, during wartime, employed. In many ways, given the harsh requirements of war fighting, cyberwar is more demanding than netwar. Operational security, deception, electronic warfare, psychological operations, and actual destruction are very demanding military activities. Cyberwar, as it is likely to be the combat form of the future, will be supported politically. The resources, organization and training needed for cyberwar will be provided once its war winning potential is grasped by the national political leadership. This development is certainly prudent. On the other hand, many of the same tools and techniques can be applied to netwar or Information War strategy. This may not be prudent as there are serious reasons to doubt the ability of the United States to prosecute Information War successfully.

First, at the level of *pragmatic* communication, the United States, as an open society, may be too vulnerable to engage in netwar with an adversary prepared to "fight back."[19] The communications infrastructure, the information highway is "wide open" in our society. American society may be terribly vulnerable to a *strategic* netwar attack in the

context of the pragmatic function of communication. The domestic computer, communication, and information networks essential for the functioning of the society are vulnerable to penetration, manipulation, or even destruction by determined "hackers" who, in the future, may not be anarchic amateurs but well-paid network-ninjas inserting the latest Bulgarian/Rumanian virus into Compuserve or Internet. Prudence suggests saying little more on this point. A *strategic* information warfare attack on the nation's pragmatic communication functions could have strategic effect.

If the goal of pragmatic communication is merely behavior modification devoid of substantive or moral consideration, and if, as appears to be true, our "open" society resists all attempts at "censorship," the opportunity for "benign" attempts to manipulate perceptions and shape American public opinion by little-regulated foreign lobbying interests, whether governmental, business, or "private," is, again, a vulnerablity. Currently, for example, there are over 14,000 data-bases on Internet accessible and used by over 20 million people world-wide. Infosphere dominance, then, may be as complex and elusive as "escalation dominance" appeared to be in nuclear strategy. It will certainly be expensive. The US armed forces devote ever more resources and attention to computer and data-base security. The resources required for cyberwar are not insignificant; the requirements and resources for a national Information War strategic capability would be massive and, given competing demands for welfare over warfare, unlikely to be made available.

Second, the political and legal issues are unclear. While theoretically a requirement to develop or implement a national Information War strategy could be communicated from the President to the executive branch agencies such as the Departments of State, Justice, Defense, the Central Intelligence Agency, and other executive agencies, it is unclear whether there is adequate Congressional oversight. Which committees of the House or Senate would have oversight of policies attendant to Information War or, for example,

inquire into the judgment of a local Joint Force Commander or CINC who wished to use the tools of cyberwar for a benign netwar attempt at perception manipulation in peacetime to shape the potential wartime environment? The US armed forces execute the national military strategy, they do not make it. The US armed forces are developing, quite appropriately, the tools, techniques and strategy for cyberwar or C2W to execute the national military strategy and, consequently, albeit unintentionally, the capabilities to execute a national Information War strategy. The former is their job under the Constitution; the latter may not be.

Finally, Information War, a "societal-level ideational conflict waged in part through internetted modes of communication," may be beyond the philosophical competence of the executive agencies and the current political class who would have to determine the *substantive content* to be communicated. From the perspective of "modern" secular, liberal society, multicultural pluralism is the single greatest strength of American society. While diversity may make the formation and execution of domestic and even foreign policy more complex, many would argue that the lack of a moral center of gravity or public philosophy in American society renders America nearly impervious to any substantive *strategic* level Information War attack or manipulation by hostile foreign states or interests. American public substantive communication concerns contending secular "visions" of America. For some, utilitarian enlightened self-interest is the "substance" of the "good" society. For others, liberal individualism, technological progress, ethno-nationalistic racialism, or self-actualization is the public project. And, as "Moral Reason," in the classical or religious sense of the distinctively human mode of moral discourse, has been replaced by "scientific rationality" seen as the pragmatic coordination of ends and means, even a national security strategy of Information War could be developed to relate resources and effort to ends which are beyond substantive moral debate.

A concrete human society targeted for Information War aimed at influencing the "emotions, motives, objective reasoning, and ultimately the behavior" of either leaders, citizens, or subjects is still a little universe of substantive conversation "illuminated with meaning from within by the human beings who continuously create and bear it as the mode and condition of their self-realization." The technological wizardry does not change the humanity of the target. Unless the goal of Information War is merely the use of *pragmatic* communication to unhinge people from their ability to reason objectively, and consequently create an interesting problem for post-conflict reconstruction, any netwar or Information War must communicate a *substantive* replacement for the discredited *substantive* content of the target society.

If, say, an Information War were to be mounted against China to disrupt its drive for regional hegemony, the goal would be to "withdraw the Mandate of Heaven" from the rulers and "influence" the Chinese leaders and people to adopt the behavior we find appropriate. Put in terms of such a concrete policy goal, the problematic nature of Information War becomes obvious. Does anyone in the executive agencies or among the political class *really* believe that we know the *substantive* discourse of China sufficiently well to withdraw the Mandate of Heaven? Worse: does anyone really believe that we have the philosophical sophistication to project an alternative substantive discourse to replace, convincingly, the emotions, motives, reasoning, and behavior grounded in the Chinese reality we propose to "influence?" We *might* be able to *destroy* their objective reasoning through a "successful" Information War. We might indeed be able to loose mere anarchy in a society, but that is not usually the *political* goal of war-fighting.

In *operational*-level cyberwar or C2W the goal is to exploit the evolving stochastic and unpredictable enemy actions by superior ability to deploy power assets. At the *strategic* level, netwar or Information War is not a prudent national security or military

strategy for the simple reason that neither the armed forces nor any other instruments of national power have the ability to exploit a society to guarantee either advantageous or *predictable* results. "Societal-level ideational conflict" may need to be considered with all the care given to the conduct of nuclear war as the "end state" of netwar may not be bloodless surrender, but total destruction of the targeted society. Conflict resolution, including ending wars this side of blasting people into unconditional surrender, assumes and requires *rationality* -- even the debased rationality of mere scientific coordination of ends with means. Moral reasoning and substantive communication are not required; minimal reasoning and pragmatic communication *are* required. The successful strategic-level Information War may, however, have destroyed even minimal reasoning and pragmatic communication in the target society.

On the assumption that it was not the goal of US policy to totally destroy the Soviet Union, the "decapitation" of the Soviet military leadership in a hypothetical nuclear exchange was to defend the United States by preventing an escalatory or retaliatory nuclear strike. Precisely how war-termination would have been accomplished will remain, hopefully, one of the great mysteries. The "decapitation" of the leadership as the target of an Information War is to be accomplished by successful "meta-propaganda." That is, the credibility, legitimacy, or even physical ability to communicate of the leadership/decision-makers is compromised or destroyed relative to their own population and in terms of their own epistemology. With whom, then, do we negotiate the end of the conflict? What confidence do we have that their decision, even if communicated to the people, would be accepted as "real" and not another "virtual" event? And, depending on the content, intensity and "totality" of the Information War, the political equivalent of psychological "inflation" is a genuine possibility; personalities are, as C.G. Jung observed, "flooded" with irrational or unconsciousness factors. "The clinical consequence is generally an acute psychosis."[20] How do we do war-termination or conflict resolution while simultaneously

multiplying the number of psychotics and others whose "objective reasoning" has been compromised, at best?

As the destructive effects of nuclear war were recognized by rational decision-makers as disproportionate with the goals of almost any imaginable conflict, likewise, the destructive effects of a "total" Information War assault on the humanity and the rational foundation of communication in society may be disproportionate with the any rational political goals of the conflict. As Sun-Tzu observed, "without advantage, do not act; without gain, do not utilize; without crises, do not battle."[21] Controlling the power evolution to impose the commander's battlefield order on stochastic chaos *may* be possible in operational cyberwar. Controlling the power evolution "imposed as a form on the remnants of societies no longer capable of self-organization" because their *substantive* universe of meaning has been destroyed *may*, on the other hand, *not* be possible.[22] The attempt, however, is the very essence of Imperialism.

finis

ENDNOTES

[1] Alvin & Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, (Boston: Little, Brown & Co., 1993).
[2] Alvin & Heidi Toffler, *ibid.*, p.141.
[3] Bruce Sterling, *Islands in the Net*, (NY: Ace Books, 1988).
[4] John Arquilla & David Ronfeldt, "Cyberwar is Coming," *Comparative Strategy*, Vol.12 (1993), pp. 141-165.
[5] Arquilla & Ronfeldt, *ibid.*, p.144.
[6] John A. Warden, *The Air Campaign: Planning for Combat*, (Washington, DC: National Defense University Press, 1988), p.129, ff.
[7] Alvin & Heidi Toffler, *War and Anti-War*, p.167.
[8] Alvin & Heidi Toffler, *ibid.*, p.173.
[9] Alvin & Heidi Toffler, *ibid.*, p.168.
[10] Alvin & Heidi Toffler, *ibid.*, p.168.
[11] Eric Voegelin, "Necessary Moral Bases for Communication in a Democracy," in: Marquette University Press, *Problems of Communication in a Pluralistic Society*, (WI: Marquette University Press, 1956), pp.53-68.
[12] Eric Voegelin, *The New Science of Politics*, (IL: The University of Chicago Press, 1952), p.27.
[13] Voegelin, "Moral Bases...", p.58.
[14] Arquilla & Ronfeldt, "Cyberwar is Coming," p.155.
[15] George E. Orr, *Combat Operations C3I: Fundamentals and Interactions* (Maxwell Air Force Base, AL: Air University Press, 1983), p.47 and *passim*.
[16] John R. Boyd, *A Discourse on Winning and Losing* (unpublished manuscript).
[17] Sun-Tzu, *The Art of War*, J.H. Huang, trans. (NY: Quill, 1993), p.68.
[18] Sun-Tzu, *ibid.*, p.109.
[19] Jean Pichot-Duclos, "Toward a French 'Economic Intelligence' Model," *Defense Nationale* (Jan. 1994), pp.73-85 in: Federal Broadcast Information Service - West Europe (25 January 1994), pp.26-31.
[20] "Inflation," *Encyclopaedia of Psychology*, (NY: Herder & Herder, 1972), Vol.2, p.121.
[21] Sun-Tzu, *The Art of War*, p.110.
[22] Eric Voegelin, *Order and History*, Vol. IV - "The Ecumenic Age," (LA: Louisiana State University Press, 1974), p.117.