Information War - Cyberwar - Netwar

George J. Stein

[Table of Contents][Chapter 7]

In Arthur Waley's *Three Ways of Thought in Ancient China*, Chuang Tzu tells the story of a simple gardener who was shown a new tool that promised to change gardening. He laughed scornfully and replied,

I used to be told by my teacher that where there are cunning contrivances there will be cunning performances, and where there are cunning performances there will be cunning hearts. He in whose breast a cunning heart lies has blurred the pristine purity of his nature; he who has blurred the pristine purity of his nature has troubled the quiet of his soul, and with one who has troubled the quiet of his soul Tao will not dwell. It is not that I do not know about this invention; but that I should be ashamed to use it.[1]

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."[2] 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 (e.g., the president and the Congress) and, in dealing with foreign states or groups, executed by the Departments of State, Commerce, Agriculture, etc.

Policies for developing and using military forces are formulated by the national political authorities and conveyed to the armed forces through the secretary of defense. Few, however, have paid much attention to just how and by whom psychological forces are to be developed to support national policies. More importantly: What are psychological forces? By whom will these forces be used? With what authority? To what ends?

New tools and technologies for communication have created the potential for a new form of psychological warfare to a degree imagined only in science fiction. This new form of warfare is known as "information warfare." When we come to know the Tao of such an invention as information warfare, we may find that we are ashamed to use it.

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." Such a strategy would include clear doctrine, and a policy for how the armed forces will acquire, process, distribute, and project knowledge.[3]

Quoting from the "Memorandum of Policy No. 30" (6 May 1993) of the US Joint Chiefs of Staff, the Tofflers argue that the US military is expanding the concept of Information War to include psychological operations aimed at influencing the "emotions, motives, objective reasoning, and ultimately the behavior" of others. Such an expansion would mirror the evolution of traditional warfare toward Information War. It would also mirror the progrssive steps of generating wealth from agriculture and natural resources in much earlier times, to the nineteenth and early twentieth century emphasis on industrial production, to the present emphasis on generating information products as a major new source of income.

As "first wave" wars were fought for land and "second wave" wars were fought for control over productive capacity, the emerging "third wave" wars will be fought for control of knowledge. And, since "combat form" in any society follows the "wealth-creation form" of that society, wars of the future will be increasingly "information wars."

Currently, there is neither formal military doctrine nor official definitions of information warfare. Despite the computer jargon involved, the idea of information warfare has not only captured the attention of military analysts—it also poses important policy questions.[4]

Despite the lack of authoritative definition, "netwar" and "cyberwar" are emerging as key concepts in discussing Information War. Originally these ideas seem to have come from the science fiction community. Consider, for example, the thought-provoking future war suggested in Bruce Sterling's *Islands in the Net*.[5] More recently, the concepts of netwar and cyberwar have been developed by John Arquilla and David Ronfeldt in their important essay, "Cyberwar is Coming!"[6] Their suggestions provide a thoughtful starting point for exploring the issues that surround "information war."

Netwar, according to them, is a societal-level ideational conflict waged in part through internetted modes of communication. That is, netwar is most likely to be a nation-against-nation strategic level conflict. Netwar is about ideas and epistemology— what is known and how it is known. It would be waged largely through a society's communication systems.

The target of netwar is the human mind. One could argue that certain aspects of the cold war had the characteristics of a dress rehearsal for future netwar. Consider, for example, Radio Free Europe, the Cominform, Agence France Presse, or the US Information Agency. But netwar may involve more than traditional state-to-state conflict. The emerging of nonstate political actors such as Greenpeace and Amnesty International, as well as survivalist militias or Islamic revivalists, all with easy access to worldwide computer networks for the exchange of information or the coordination of political pressure on a national or global basis, suggests that the governments may not be the only parties waging Information War.

At first glance, netwar may appear to be a new word for old-fashioned propaganda. It would be comforting to believe that the "tried and true" methods (and limitations) of

propaganda still worked. And the Gulf War showed that both Saddam Hussein and the Alliance were still of the old school. The war contained many elements of classic propaganda: accusations of bombed baby-milk factories and stolen baby incubators, inflated rhetoric and inflated stakes of the conflict; the future of the new world order and "the mother of battles" for the future of Islam; and the classic "us or them" polarization in which "neutrality" or unenthusiastic support was decried.

One element of traditional propaganda was absent, however, while Saddam Hussein became the "new Hitler" and President Bush was the "Great Satan," there was little demonization or dehumanization of the opponent. Perhaps the multicultural nature of the American-led alliance precluded turning the Iraqi army into something subhuman. Indeed, there may have been a spark of netwar genius in treating the Islamic Iraqi soldiers as "brave men put into an impossible situation by a stupid leader." Under such conditions, there is no dishonor in surrendering. And there may have been a glimpse of future netwar—it is rumored that Baghdad Radio signed on one morning with "The Star-Spangled Banner."

Traditional propaganda was usually targeted to influence a mass audience. Contemporary technologies have the potential to customize propaganda. Anyone who has received individually targeted advertising from a company specializing in "niche" marketing has had a momentary shudder upon realizing that some private companies seem to know everything about our tastes and buying habits.

Contemporary databases and multiple channels for information transmission have created the opportunity for custom-tailored netwar attacks. Computer bulletin boards, cellular telephones, video cameras tied to fax machines—all provide entry points and dissemination networks for customized assault.

A major new factor in information war results directly from the worldwide infosphere of television and broadcast news. Many people have begun to realize that governmental decisions are becoming increasingly reactive to a "fictive" universe created by, CNN and its various international competitors. This media-created universe is dubbed "fictive" rather than "fictional" because while what is shown may be "true," it is just not the whole, relevant, or contextual truth. And, of course, the close etymological relationship between "fictive" and "fictional" suggests how easy it is to manipulate the message.

Nevertheless, this fictive universe becomes the politically relevant universe in societies in which the government or its military is supposed to "do something." 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. There were no reporters with "skylink" in Sudan because the government of Sudan issued no visas. The potential for governments, parties in a civil war such as Bosnia, rebels in Chiapis, or even nonstate interests to manipulate the multimedia, multisource fictive universe to "wage societal-level ideational conflicts" should be obvious.[7]

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 niche-manipulation potential available to states or private interests with access to the universe of internetted communications such as the networks over which business, commercial, or banking information are transmitted to suggest that "Mexico" is about to devalue the peso could easily provoke financial chaos. The target state would not know what had happened until too late.[8]

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. To put it in the jargon of the infowarriors, info-niche attack in an increasingly multisource fictive universe offers unlimited potential for societal-level netwar.

Pictures Worth A Thousand Tanks

When the new, but already well-understood, simulation technologies of the Tekwar and MTV generation are added to the arsenal of netwar, a genuinely revolutionary transformation of propaganda and warfare becomes possible. Traditional propaganda might have attempted to discredit an adversary's news media showing, for example, that as the official casualty figures were demonstrably false, 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.

Today, 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, but by the time the people of the targeted nation discover that the nationwide broadcast of the conversation between the maximum leader and "Jimmy Carter" in which all loyal citizens were told to cease fighting and return to their homes was created in Hollywood or Langley, the war may be over. Netwar is beginning to enter the zone of illusion.

This is not science fiction; these are the capabilities of existing or rapidly emerging technologies. Here's how it might work: through hitching a ride on an unsuspecting commercial satellite, a "fictive simulation" is broadcast. Simultaneously, various "info-niches" in the target state are accessed via "the net." These info-niche targets, and the information they receive, are tailored to the strategic needs of the moment: some receive reinforcement for the fictive simulation; other receive the "real" truth; others receive merely slight variations. What is happening here?

This kind of manipulation elevates the strategic potential of infopropaganda to new heights. This is not traditional propaganda in which the target is discredited as a source of reliable information. Rather, the very possibility of "truth" is being replaced with "virtual reality"; that is, "information" which produces effects independent of its physical reality. What is being attacked in a strategic level netwar are not only the emotions, or motives, or beliefs of the target population, but the very power of objective reasoning: this threatens the very possibility of state control.

Let us return to the previous scenario to play out its effects. The fictive simulation of the maximum leader's call to stop fighting would, of course, be followed immediately by a "real" broadcast in which state "Voice and Vision" exposes the netwar attack as propaganda invented by "culture destroyers in Hollywood." "Jimmy Carter" is denounced as a hoax. But the damage has already been done: it is all but impossible for the television viewers of the targeted state to tell which broadcast is true and which fiction, at least in a timely manner. In a society under assault across its entire infosphere, it will become increasingly difficult for members of that society to verify internally the truth or accuracy of anything. Objective reasoning is threatened.

At the strategic level, the ability to "observe" is flooded by contradictory information and data; more importantly, the ability to "orient" is weakened by the assault on the very possibility of objective reasoning; "decisions" respond increasingly to a fictive or virtual universe and, of course, governmental or military "actions" become increasingly 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 by attacking his ability to form a coherent strategy.[9]

Reality, however, may be far more complex than the infowarriors yet imagine, and victory not so neat. The idea of "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 disruption of the targeted society. Victory may be too costly as the cost may be truth itself.

What Is Truth?

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 using the techniques of information warfare at the strategic level is compatible with 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, more importantly, the practical ability to develop

and deploy the techniques of information warfare at the strategic level in a prudent and practical manner. There are good reasons 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.[10] 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. Simply, it is the glue which binds a society together.

At the most trivial level, the moral purpose of substantive communication can be seen in contemporary American efforts to remove sexist or racist language from accepted use. At a more serious level, the debates in American society about prayer in the public schools illustrate a recognition of the substantive and formative nature of communication in society, as "private religious views," in the view of many, must not corrupt the public school formation of character for life in pluralistic, modern America.

Finally, any real world society rests on the substantive communication and understanding among its members. Again, in Voegelin's terms, society is no mere external structure of relationships; it is a "cosmion," a universe of meaning "illuminated with meaning from within by the human beings who continuously create and bear it as the mode and condition of their self-realization."[11]

The efforts of several nations such as China, Iran, or Saudi Arabia to insulate their societies from the effects of the global communications network illustrate their awareness that their cultures and societies may depend on a shared, substantive universe of discourse distinctive to their societies.

Even within the West, the French believe 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.[12] That France seeks to limit the percentage of foreign broadcast material and American films in Europe illustrates the seriousness with which they consider the substantive nature of communication.

Voegelin's second construct, identifying the pragmatic function of communication in society, is reasonably straightforward. Pragmatic communication is defined by its goal and consists of the universe of techniques designed to influence 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 intends to mold perception, and consequently behavior, to the purposes of the communicator. This pragmatic use of communication as an attempt at perception manipulation is, of course, the central essence of information war. Its use by the government and the armed forces is, consequently, the real issue.

Finally, the intoxicant function of communication in American society is equally straightforward. The addiction of a considerable part of the citizenry to talk shows, soap

operas, romance novels, professional sports broadcasts, high-profile legal trials and other well-known forms of distraction and diversion is well catered to by the entertainment industry.

For Voegelin then, civil communication or public discourse in contemporary American society is dominated almost entirely by the intoxicant and pragmatic modes. More importantly, the absence of substantive communication in public life is defended by much of the secular and liberal political class in the name of freedom, pluralism, and multiculturalism.

Pluralistic America is supposed to be a society in which the formation of character or opinion is left, through the use of various means of communication, to private initiative. Government attempts at "communication" in an information war, especially if prosecuted by the armed forces, would raise serious questions in a pluralistic, multicultural society.

The official military view of 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."[13]

Strategy is the means to achieve an end, with military strategy serving political or policy purposes. A slightly different view of strategy, however, may highlight a problem of Information War. If strategy were seen as "a plan of action designed to achieve some end; a purpose together with a system of measures for its accomplishment," the limitations of infowar thinking are obvious.[14]

Sound military strategy requires influencing the adversary decision maker in some way that is not only advantageous but reasonably predictable. The goal is control, not chaos. 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 command-and-control warfare campaign to decapitate the enemy's command structure from its body of troops may or may not be "advantageous" but, more importantly, is unlikely to produce effects that are reasonably predictable.

Conflict is about a determinate something, not an indeterminate anything. If the goal of influencing the adversary's ability to "observe" by flooding him with corrupted or contradictory information and data; disrupting his ability to "orient" by the elimination of the possibility of objective reasoning; and forcing his "decisions" to respond to a fictive or virtual universe, "actions" will, of course, be produced, but they may well be actions which are chaotic, random, nonlinear and inherently unpredictable by our side as there is no "rational" relationship of means to ends.

In the context of military operational-level cyberwar or command-and-control warfare, this appeals to the infowarrior an attractive military strategy. The inherently

unpredictable nature of combat, the notorious "fog and friction" of real battle, will be amplified for the enemy in a successful cyberwar.

A successful cyber-strategy depends on the ability of the local military commander to deploy his power assets, especially his combat forces, not merely to dominate the enemy decision cycle (which, after all, has just been rendered chaotic), but to exploit opportunities as they evolve unpredictably from the disoriented, decapitated, or irrational enemy actions. Whether, then, command-and-control warfare can "shape" the battlefield or will merely generate chaos remains to be seen.

Cyber-strategy is the control of the evolution of the battlefield or theater power distribution to impose the allied 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."[15] The threat exists, however, that the destruction of enemy rationality may collapse "battle" into mere "fighting" with no outcome but surrender or death. Merely defeating hostile fielded military forces may be insufficient.

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'."[16] Whether the recent Gulf War was a strategic victory or mere "battle" remains for historians to judge. Operational-level cyberwar may, then, be that very "acme of skill" which reduces the enemy will without killing. On the other hand, it may also be the abolition of strategy as it attacks the very rationality the enemy requires to decide for war termination.

Strategic Implications

The tools, techniques and strategy for cyberwar will be developed and, during wartime, should be employed. In many ways, cyberwar is more demanding than netwar. But the resources, organization, and training needed for cyberwar will be provided once its war-winning, and casualty-reducing, potential is grasped by the national political leadership. Such a development would certainly be prudent. On the other hand, many of the tools and techniques of battlefield cyberwar can be applied to netwar or strategic-level information war. This application may not be prudent, however, as there are serious reasons to doubt the ability of the United States to prosecute information war successfully.

One reason is that the United States is an open society; it may be too vulnerable to engage in netwar with an adversary prepared to "fight back." [17] The communications infrastructure, the "information highway," is "wide open" in our society. American society may be terribly vulnerable to a strategic netwar attack; getting us to believe fictive claims appears to be what commercial and political advertising are all about, and they seem to be effective. Also we may find physical control and security to be impossible. The domestic computer, communication, and information networks essential for the daily functioning of American society are very vulnerable to penetration and manipulation—even destruction—by determined hackers.[18] In the future, these may not

be amateurs but well-paid "network ninjas" inserting the latest French, Iranian, or Chinese virus into Compuserve or other parts of the internet.[19]

A strategic information warfare attack on America's communication systems, including our military communication systems, air traffic control system, financial net, fuel pipeline pumping software,and computer-based clock/timing systems, could result in societal paralysis.

Currently, for example, over 14,000 Internet databases are being used by over 30 million people in over 90 nations. Over 1,600 software pirates are prowling the Internet, some in the employ of hostile commercial or intelligence services. The recent "spy flap" between France and the United States over alleged US attempts to gather data on French Telecom may be indicative of the future.[20]

Infosphere dominance—controlling the world of information exchange—may be as complex and elusive as "escalation dominance" appeared to be in nuclear strategy.[21] It will certainly be expensive: the US business community and the US armed forces are required to devote ever more resources and attention to computer, communications, and database security. The resources and skills required for battlefield cyberwar are not insignificant, but the resources and skills required to wage Information War at the national strategic level would be massive.

The second reason to doubt US ability to prosecute an information war is that the political and legal issues surrounding info war are murky. What of congressional oversight? Would one "declare" information war in response, say, to an Iranian-originated computer virus assault on the FBI's central terrorist database? And what about preparing for it? How should we develop and implement a national capability for netwar?

While theoretically a requirement to develop or implement a national information war strategy, analogous to the nuclear-era single integrated operations plan, could be communicated from the president to the executive branch agencies, it is unclear whether there would be adequate congressional oversight. Which committees of the House or Senate would have control and oversight of policies attendant to information war, and which would have the power to inquire into the judgment of a local ambassador or military commander who wished to use the tools of cyberwar for a perception manipulation in peacetime that would shape the potential wartime environment?[22]

The US armed forces only execute the national military strategy—they do not control it. However, they are developing, quite appropriately, the tools and techniques to execute the national military strategy for operational-level cyberwar. They are simultaneously, albeit unintentionally, developing the tools and capabilities to execute a national strategic information war strategy. The former is their job under the Constitution; the latter may not be. Congressional oversight in the development of a national strategic-level information war capability is even more essential than oversight of the intelligence community.

The third reason to doubt US capabilities in prosecuting an effective information war is that such a "societal-level ideational conflict waged in part through internetted modes of communication" may simply be beyond the competence of the executive agencies that would have to determine the substantive content to be communicated. Pluralism is a great strength of American society, but perhaps a drawback in waging information war.

While diversity may make the formation and execution of domestic and even foreign policy more complex, the lack of a moral center or public philosophy in American society could render the political leadership incapable of building a consensus on strategic-level information war policies. And, since there is no single view of what is morally acceptable, but simply a host of contending views, a national security strategy of information war could be developed by the national security decision makers that lacked a moral consensus.

The technological wizardry does not change the humanity of the target. Unless the goal of information war is merely to unhinge people from their ability to reason objectively, and thereby create an interesting problem for post-conflict reconstruction, any strategic-level netwar or information war would seem to require the ability to communicate a replacement for the discredited 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 policies or behavior we find appropriate.

Put in terms of such a concrete policy goal, the philosophically problematic nature of information war becomes outrageously obvious. Does anyone really believe that the US national executive agencies, including the armed forces and the Central Intelligence Agency, know the substantive discourse of China sufficiently well to withdraw the Mandate of Heaven?

The final reason, then, can be stated in the form of a question: does anyone really believe that anyone in the US government has the philosophical sophistication to project an alternative discourse to replace the emotions, motives, reasoning, and behavior grounded in the Chinese reality we propose to influence? Would our "fictive" creation really have "virtual" effects. We might be able to use the armed forces or the CIA to destroy China's objective reasoning through a "successful" information war. Indeed, we might be able to loose anarchy in a society, but that is not usually the political goal of war.

Second Thoughts

The techniques being developed by the armed forces for a more narrowly constrained operational-level cyberwar was demonstrated in the Gulf War. Translated to the strategic level, however, 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 an adversary's society in a way that promises either advantageous or predictable results.

Societal-level ideational conflict" must be considered with all the care given to the conduct of nuclear war, as the "end state" of a netwar may be total disruption of the targeted society. Conflict resolution, including ending wars this side of blasting people into unconditional surrender, assumes and requires some rationality—even if that rationality is the mere coordination of ends with means.

Moral reasoning and substantive communication may not be required; minimal reasoning and pragmatic communication are required. However, a successful all-out strategic-level information war may, however, have destroyed the enemy's ability to know anything with certainty and, thereby, his capacity for minimal reasoning or pragmatic communication.

In some exercises during the cold war "decapitation" of the Soviet military leadership in a hypothetical nuclear exchange was intended to defend the United States by preventing an escalatory or exploitative strike, nuclear or otherwise. Precisely how war termination would have been accomplished without an effective leadership will remain, hopefully, one of the great mysteries. The "decapitation" of the leadership is, however, often proposed as a key goal of an information war. That is, the credibility and legitimacy—even the physical ability to communicate—of the decisionmakers will be compromised or destroyed relative to their own population and in terms of their own worldview. And even if we merely "seize" his communication system electronically and substitute our "reality" into his society, with whom, then, do we negotiate the end of the conflict?

What confidence do we have that a call to surrender, even if communicated to the people by either the enemy leadership or our "net warriors," would be accepted as "real" and not another "virtual" event? And, depending on the content, intensity, and "totality" of a strategic information war, personalities could be flooded with irrational or unconsciousness factors—the clinical consequence of which is generally acute psychosis. How do we accomplish conflict resolution, war termination, or postconflict reconstruction with a population or leadership whose "objective reasoning" has been compromised?

Just as the mutually destructive effects of nuclear war were disproportionate to the goals of almost any imaginable conflict, so may be the mutually destructive effects of a "total" information war exchange on the publics exposed and subsequent rational communication between the sides. And as the techniques of "cyberstrike" proliferate throughout the world, enabling small powers, nonstate actors, or even terrorist hackers to do massive damage to the United States, "mutually assured cyberdestruction" may result in a kind of infowar deterrence. As Sun-Tzu advised, "without advantage, do not act; without gain, do not utilize; without crises, do not battle."[23]

Information War, then, may be the central national security issue of the twenty-first century. Therefore, the United States must develop a coherent national-level policy on the

military and strategic use of new information warfare technologies. To facilitate this objective, the US armed forces are developing, under the rubric of command and control warfare, the technologies and systems that will provide the capability for "cyberwar."

It may be possible to control and exploit information so as to purposely generate stochastic chaos, though there are some doubts.[24] Many of the same technologies and systems can be used to develop a national-level capability for strategic "netwar." Here, however, there are genuine doubts. As Voegelin feared, it may not be possible to control and exploit information and information technologies to impose "a form on the remnants of societies no longer capable of self-organization" because their substantive universe of meaning has been destroyed or corrupted.[25]

Few info-warriors would claim the ability to "reorient" the former Soviet Union into a liberal society, or to influence the far more ancient barbarism in that heart of darkness, Rwanda. Perhaps strategic-level information war is, indeed, like nuclear war: the capability is required for deterrence; its employment, the folly of mutually assured destruction. But if the United States is to develop the capacity for information war, in the sure and certain knowledge that the technologies have already "proliferated" to both state and nonstate potential rivals, a realistic national consensus must be built.

It is useless to pretend that the proliferation of these technologies will not provide capabilities that can do serious harm. It is useless to pretend that military-based command and control warfare capabilities will not be developed, and it is useless to pretend that cyberwar technologies could not be turned to netwar applications. It is almost universally agreed that these capabilities are essential on the contemporary battlefield.

It is essential, then, that the president and the Congress give serious and sustained attention to cyberwar, netwar, and information war.