Disclaimer

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

A THEORY OF INFORMATION WARFARE

Preparing For 2020

COL RICHARD SZAFRANSKI

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

THE PROFESSION of arms in a democracy is not exempt from oversight or from consideration of just conduct, even in warfare. Where the will of the people, the moral high ground, and the technological high ground are the same, the profession will remain a useful and lofty one. If, however, the moral high ground is lost, a domino effect occurs: public support is lost, the technological high ground is lost, and the armed forces are lost. It is within this framework that this article postulates a theory of information warfare[1] within the larger context of warfare and proposes ways to wage information warfare at the strategic and operational levels. The tools to wage information warfare are at hand, and because information weapons are such powerful weapons, both combatants and noncombatants need to be protected against them. The vulnerability to information warfare is universal. The decisions to pursue the development of information weapons or to prosecute information warfare are governmental decisions. These decisions need to be made consciously and deliberately and with an understanding of the moral and ethical risks of information warfare. After assessing all the risks and deciding to create information weapons or engage in information warfare, the decision makers should first have an understanding of these weapons and a weapon employment theory before such warfare starts rather than after the weapons are deployed or have already been employed.

Information

Information as used here means the "content or meaning of a message."[2] An aim of warfare always has been to affect the enemy's information systems. In the broadest sense, information systems encompass every means by which an adversary arrives at knowledge or beliefs. A narrower view maintains that information systems are the means by which an adversary exercises control over, and direction of, fielded forces. Taken together, information systems are a comprehensive set of the knowledge, beliefs, and the decision-making processes and systems of the adversary. The outcome sought by information attacks at every level is for the enemy to receive sufficient messages that convince him to stop fighting.

Why would an adversary stop fighting? There are a number of possibilities: an inability to control fielded forces, demoralization, the knowledge or belief that combat power has been annihilated, or an awareness that the prospects of not fighting are superior to the prospects of continuing the fight. These "stop-fighting" messages might be as varied in content or meaning as "Cannae has ruined you," or "Submit to the Tartar or die," or "Your counterattack has failed," or even "Your own people do not support you in warfare that kills babies." Although the methods of communicating the stop-fighting

19970730 102

DTIC QUALITY INSPECTED 2

New Text Document.txt

Today Date:24 July 1997

This paper was downloaded from the Internet.

Distribution Statement : A

POC:Air University Maxwell Air Force Base
US Air Force

message have changed over the years, the meaning of the message itself remains fairly constant: stop fighting.

As social institutions evolved from first-wave agrarian societies to second-wave industrial states, information systems evolved and decision-making processes became more complex. Mercantile organizations arose within or alongside the dominant political structures, adding elements of greater complexity as the scope of their activities enlarged. Knowledge networks of knowledge workers, the newest form of institutional structure, emerged and their numbers increased in tandem with the availability of the tools of information technology. As information technology advanced, information systems allowed knowledge, or know-how, to make all the other institutional forms more effective.[3]

As societal institutions evolved, the ways in which societies fought evolved also. The terrorizing drums, banners, and gongs of Sun Tzu's warfare, aided by information technology, became the sophisticated psychological operations of modern warfare. The aim of warfare moved from, or could move from, exhaustion to annihilation to control, according to John Arquilla and David Ronfeldt.[4] Information technology may now have evolved to the point where "control" can be imposed with little physical violence or bloodshed. On the surface this appears to be a good thing. At its center, it may be a dangerous thing. Closer scrutiny should reveal which of these is the case.

What Warfare Is

Warfare is the set of all lethal and nonlethal activities undertaken to subdue the hostile will of an adversary or enemy. In this sense, warfare is not synonymous with "war."[5] Warfare does not require a declaration of war, nor does it require existence of a condition widely recognized as "a state of war." Warfare can be undertaken by or against state-controlled, state-sponsored, or nonstate groups.

Warfare is hostile activity directed against an adversary or enemy. The aim of warfare is not necessarily to kill the enemy. The aim of warfare is to merely subdue the enemy. In fact, the "acme of skill" is to subdue an adversary without killing him.[6] The adversary is subdued when he behaves in ways that are coincident with the ways in which we_the aggressor or the defender_intend for him to behave.[7] In aiming to subdue hostile will, we must have a clear understanding of the specific nonhostile behaviors we intend to compel, or the hostile ones we want to prevent.

When the security forces of a state engage an enemy state in warfare, the government determines the specific nonhostile behaviors sought from the adversary. When other groups_guerrillas, gangs, clans_engage in warfare, the group leader decides the specific nonhostile behaviors sought. In both state and nonstate warfare forms, the decisions made by group leaders define the aims, the methods, and the desired postconflict conditions of the warfare. Even so, it is a fiction, albeit a common and convenient one, to assert that "states" or "groups" wage warfare. The decision to engage in warfare, including the decision to terminate warfare, is made by *leaders* in the state or group. Likewise, it is the hostile will of enemy leaders that must be subdued to be successful in warfare.[8] Group members, or the citizens of states, may influence the leaders' decisions, but it is the hostile will of leadership that must be subdued. If the "mandate of heaven" passes from the leader to other group members_successor leaders or the population at large_the hostile will of these new leaders must be subdued. Information warfare can help withdraw the mandate of heaven from the hands of adversary leaders.

The great discovery that launched the information age was awareness that everything in the external world could be reduced to combinations of zeroes and ones. These combinations could be transmitted electronically as data and recombined upon receipt to form the basis of information. According to the

seminal work on control warfare by Arquilla and Ronfeldt, information is more than the content or meaning of a message. Rather, information is "any difference that makes a difference."[9] Information warfare is a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs. Information warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities_a netwar or cyberwar_or it can be undertaken as the sole form of hostile activity.[10] Most *weapons*_a word used to describe the lethal and nonlethal tools of warfare_only have high utility --against external adversaries. While most often employed against external adversaries, many of the weapons of information warfare are equally well suited for employment against internal constituencies. For example, a state or group would not normally use guns and bombs against its own members; however, the weapons of information warfare can be used, have been used, and very likely will be used against both external and internal adversaries. Information warfare in the Third Reich, for example, was omnifrontal.

Information warfare is hostile activity directed against any part of the knowledge and belief systems of an adversary. The "adversary" is anyone uncooperative with the aims of the leader. Externally, this is the agreed-upon "enemy," or the "not us." Internally, the adversary might be the traitor, the faint of heart, or the fellow traveler_anyone who opposes or is insufficiently cooperative with the leader who controls the means of information warfare. If the internal members of a group are insufficiently supportive of the aims of the leader during warfare, internal information warfare (including such things as propaganda, deception, character assassination, rumors, and lies) can be used in attempts to make them more supportive of the aims of leadership.

Warfare and Its Relation to What We Know or Believe

Whether directly employed against an external adversary or internal constituencies, information warfare has the ultimate aim of using information weapons to affect (influence, manipulate, attack) the knowledge and belief systems of some external adversary. It is useful in warfare, for example, for an external adversary to know, or at least believe, that the opposing state or group is united against him or her. Information warfare, simultaneously employed to make internal constituencies cooperative and external adversaries believe its enemy is a united front, is used to help seat that awareness in the knowledge and beliefs residing in the mind of adversary leadership.

The Fragility of Knowledge and Beliefs

Knowledge systems are those systems organized and operated to sense or observe verifiable phenomenological indicators or designators, translate these indicators into perceived realities, and use these perceptions to make decisions and direct actions.[11] Sensing that the plate is hot, one releases it. Observing that one's expenditures exceed income, one curbs spending. Our sensing and observing systems allow us to *know*. We decide and act based on our knowledge, but not on knowledge alone. Knowledge systems are organized according to scientific principles and sustained by the scientific method. That is, knowledge systems are organized to collect empirical data by sensing or observation to formulate hypotheses, to conduct tests that validate or invalidate the hypotheses, and to use these findings as the basis for further action. Belief systems are those implicit or explicit orientations both to empirical data in the form of verifiable perceptions and to other data or awareness (nightmares, phobias, psychoses, neuroses, and all the other creatures living in the fertile swamp of the subconscious, the collective unconscious, or Jung's "unconscious psyche"[12]) that are not verifiable or,

at least, are less easily verifiable.[13] According to John Boyd, the process or act of orientation (what Boyd calls "the Big O" in the OODA [observation-orientation-decision-action] loop) also is influenced by genetic heritage and cultural traditions.[14] Thus, the orientation of American leaders is different than the orientation of, say, Japanese or Chinese leaders. The orientation of capitalists and their leaders is different than the orientation of socialists and their leaders.

Unlike knowledge systems, belief systems are highly individualized. Why? They include the stuff of the unconscious and subconscious, powerful elements of which others and even the bearer may be unaware. Even though the target of information warfare is the mind of enemy leadership, it is glib reductionism to think of the enemy as being of "one mind." The enemy is really many individual enemies, many minds. This only complicates the problem slightly. For example, if the enemy is dispersed, separate minds can be attacked separately, using the fact of isolation to the attacker's advantage. If the enemy is concentrated (and over half the people on the planet will live in metropolitan complexes by the year 2020 and will be accessible in large numbers by way of information technology), the attack can be prosecuted against large groups. Even so, the aim of warfare is to subdue the hostile will of leaders and decision makers. This can be done directly by attacks aimed at influencing or manipulating the leader's knowledge or beliefs or indirectly by attacking the knowledge or beliefs of those upon whom the leader depends for action. Leaders and decision makers usually are not difficult to identify in any organization hierarchy. When an organization applies power or force, that organization most often assumes hierarchical characteristics. Thus, the knowledge and beliefs of decision makers are the Achilles' heel of hierarchies.

Knowledge systems, because they are more scientific, are less influenced by culture and by irrational or nonverifiable factors than are belief systems, yet both knowledge systems and belief systems are components present in every human decision-making system.[15] What is known, including the methods by which it came to be known, can be tested by its relation to something else and determined to be valid or invalid, true or false, real or unreal. What is believed is not subject to all the same tests. Even so, beliefs are no less compelling than empirically derived knowledge. Both knowledge and beliefs affect human decision making. Since the aim of warfare is to influence adversary behavior by influencing adversary decisions, information warfare actions must be directed against both the adversary's knowledge systems and belief systems. If an adversary is organized as a coalition of multiple and cooperative centers of gravity, many culturally conditioned belief systems may exist within the coalition. These may be engaged and defeated in detail. The coalition need not be separate states or groups working as an alliance. The coalition can be the constituencies within a state or within groups. Clausewitz was correct in asserting the potential liabilities associated with allies and coalitions.[16] Moreover, leaders and decision makers of the coalition provide the most fertile targets for direct or indirect attacks.

Targeting Epistemology

The target system of information warfare can include every element in the epistemology of an adversary. *Epistemology* means the entire "organization, structure, methods, and validity of knowledge."[17] In layperson's terms, it means everything a human organism_an individual or a group_holds to be true or real, no matter whether that which is held as true or real was acquired as knowledge or as a belief. At the strategic level, the aim of a "perfect" information warfare campaign is to influence adversary choices, and hence adversary behavior, without the adversary's awareness that choices and behavior are being influenced. Even though this aim is difficult to attain, it remains the

goal of a perfect information warfare campaign at the strategic level. A successful, although not necessarily perfect, information warfare campaign waged at the strategic level will result in adversary decisions (and hence actions) that consistently mismatch or fail to support the intentions or aims of the adversary leader.

A successful information warfare campaign waged at the operational level will support strategic objectives by influencing the adversary's ability to make decisions in a timely or effective manner. Said another way, the aim of information warfare activities at the operational level is to so complicate or confound the adversary's decision- making process that the adversary cannot act or behave in a coordinated or effective way. In information warfare, the goal is to harmonize the activities taken at the operational level with those taken at the strategic level so that, taken altogether, the adversary makes decisions that result in actions that consistently support our aims by consistently failing to support the adversary's aims.

At the strategic level, the leaders contemplating an information warfare campaign need to know the answers to at least three questions. First, what is the relationship of the information warfare campaign to the larger aims of the campaign? Second, what is it we wish the adversary leaders to know or believe when the information warfare campaign is concluded? That is, what is the desired epistemological end-state and consequently the success criterion? Third, what are the best information warfare tools to employ in order to meet the established success criteria? That is, how will "means" be related to "ends"?

At the operational level, the leaders responsible for prosecuting the "grand tactics" also need the answers to some questions. Will there be any withheld targets or prohibited weapons in the information warfare attacks? Is the epistemological end-state to be reached all at once, everywhere, or are there interim states that need to be reached in specific geographical areas, in a specific sequence, or in specific sectors of information activity? The questions of "command and signal" also need to be addressed. Specifically, leaders at the operational level need to know when attacks will be terminated and the means by which the termination order will be communicated. These are important questions because information weapons, depending on the weapons used, may cause collateral damage to the attacker's knowledge and belief systems.[18] In the worst case, the adversary's response could include counterattacks against "friendly" information systems that are somehow indistinguishable from collateral damage caused by the information analog of "friendly fire." This thought requires some elaboration.

Warfare is a human social activity.[19] The workplace of warriors is society, the societies of those engaged in combat and the societies of active and passive spectator groups. Because it is a human activity_and one dependent on human action, reaction, and interaction_the outcomes of some warfare activities may be unpredictable. As Grant Hammond notes in "Paradoxes of War," if the outcomes of a war could be known in advance, there would be scant reasons for the loser to fight in the first place.[20] Moreover, there may be lag times between action and response; some outcomes take longer to develop than others. Thus, the notion that World War II was the outcome of World War I (or the peace treaty that terminated combat) may very well be true. The unpredictability, however, is not confined to the consequences of war termination. Specific actions in warfare can have specific and unpredictable reactions.

Information attacks_attacks aimed at the knowledge or belief systems of adversaries_can have consequences that are as unpredictable as attacks aimed at the physical destruction of property or combat equipment or those aimed at killing human beings. Suffice it to say that information attacks have stochastic effects and that unless these are considered and evaluated in advance, an information

attack may not have the effect ultimately desired. Worse, it may have consequences that are so undesirable that the attacker will rue that an attack was made in the first place. The notion of stochastic effects, like the notion of collateral damage, needs to be considered at both the strategic and operational levels of information warfare.

The Target Sets of Information Warfare

The more dependent the adversary is on information systems for decision making, the more vulnerable he is to hostile manipulation of those systems. Software viruses only hurt those dependent on software. Radio-electronic combat only works against forces reliant on radios or electronics. Electromagnetic pulse generators_unless the generator is a nuclear weapon_do not affect human couriers and runners. While this suggests that only postindustrial states or groups are highly vulnerable to information warfare, the opposite may be the case for two reasons. First, preindustrial or agrarian societies still have vulnerable epistemological systems. Because information warfare can be prosecuted against the adversary's entire epistemology_both knowledge systems and belief systems_even preindustrial agrarian or primitive societies are vulnerable to information warfare. Second, industrial societies, and even some advanced industrial societies, may acquire much of their telecommunications infrastructure from more advanced or postindustrial societies or groups.

By way of analogy, consider the case of the homeowner and the architect. The homeowner may not be aware of flaws in his or her residence, but the architect is aware. Likewise, the operator or "owner" of a telecommunications system designed or built by others may be unaware of important features of which only the designer or manufacturer has knowledge. If the architect is not directly subordinate or accountable to "the owner," then the potential exists for the architect to exploit the hidden features to his own advantage. In the warfare of business competition, the architect may have the means, motive, and opportunity to exploit these features to meet the objectives of the firm, whether or not the government or the state approves of these actions.

In the case of advanced societies or groups, attacks against telecommunications systems can wreak havoc with an adversary's ability to make effective decisions in warfare. Yet, one should also appreciate that an apparition in the sky, even a natural phenomenon like a solar eclipse, can be used to attack the belief systems of a less advanced group. Totems and taboos might function equally as well as the targets or the tools of information warfare against a primitive group. Thus, vulnerability to information warfare is nearly universal, the differences being only a matter of degree.

An Illustration of Complexity

Information warfare is a complex notion. It is complex because the weapons employed are and always have been as common as words, pictures, and images, even though today these may be communicated or manipulated in uncommon ways. It is complex because the attacks are crafted by minds to affect minds. In addition, it is complex because the attacks can be direct or indirect, aimed at internal or external constituencies, the only constant being the effect sought. The desired effect of information warfare is to influence and change what the adversary believes or what the adversary knows.

The Sepoy Mutiny of 1857-58 provides an example of the complexity. The mutiny reportedly was triggered by a rumor that the British were coating rifle cartridges in animal fat.[21] Contact with this fat was taboo to the Hindu and Muslim sepoys (Indian natives in the British army). Even though the cartridge coating was *not* animal fat and could be subjected to scientific tests that would result in this

knowledge, the sepoy *believed* the substance was animal fat. This belief was more compelling to the primitive sepoy than knowledge. Thus, it was belief, not knowledge, that influenced sepoy behavior and triggered a difficult struggle between the British and the Indians. This case is also illustrative of the fact that even though the use of this misinformation was directed against the British leadership, the attack was indirect. It was the sepoy leaders who started the rumor, and in so doing attacked the belief systems of both Hindu and Muslim sepoys to spur them to rebel against their British masters.

Thus, information warfare can be waged both internally and externally, by, against, or between societies or groups of varied technomic capability (a combination of advances in technology and the increase of economic wealth).[22] When waged against internal constituencies, its aim is to use those constituencies to meet the larger aim of warfare: subduing the hostile will of an external adversary. When information warfare is prosecuted externally, the object is to subdue the hostile will of external adversary leaders.

Vulnerable Sophisticates?

In states or groups with high technomic capability, the target set for information warfare at the strategic level is wonderfully rich: telecommunications and telephony,[23] space-based sensors, communications relay systems; automated aids to financial, banking, and commercial transactions; supporting power production and distribution systems; cultural systems of all kinds; and the whole gamut of hardware and software that constitutes how the adversary knows and what the adversary believes. Strategic information systems in states with high technomic capability oftentimes are mirrored by operational-level ones of equal complexity. All are vulnerable to attack.

Information warfare need not be deferred until hostility becomes open. Adversary leadership will be less likely to fight if it believes one or more of the following: that violence is bad, or that they will be without allies, or that they will face harsh sanctions should fighting erupt, or that their industrial base will not support prolonged warfare, or that their armed forces are unready. Should actual fighting break out, attacks at the operational level can harmonize with attacks at the strategic level.

The target set at the operational level is equally lucrative when the adversary has high technomic capability and relies on automated aids to fight. Hierarchical systems are most vulnerable, but even networks have control or relay nodes that are susceptible to attack. To function effectively, networks have hierarchical elements or nodes. Often these elements are invisible_embedded software protocols, filters, sort instructions, and the like.[24] That they are more difficult to attack may not make them immune to attack.

The higher its technomic capability and the greater the number of its interactions with other groups (including internal groups) or states, the greater the state or group's potential vulnerability to information warfare. The vulnerability may increase as network size increases, dependence on the information transacted increases, or the number or volume of transactions increases. Consequently, a state or group "engaged" worldwide may be exposed or vulnerable worldwide. (If the objective of engagement is a strategic campaign aimed at affecting the knowledge or beliefs of others, then those engaged are, of course, similarly vulnerable.) Democracies are no less vulnerable than totalitarian regimes, although democratic social systems, as groups, may be somewhat more fault-tolerant. By that is meant that democracies promote diversity and diversity increases the tolerance for difference. This willingness to accept diversity (and even the bizarre), the routine co-exis-tence of contradictory knowledge and different beliefs among individuals and groups, and the constant attempts at manipulation by marketing experts do not reduce the vulnerability of a democracy, but they do mitigate

the impact of information warfare attacks. Said another way, many people in democratic nations may be immune to attacks because their knowledge may be limited, their belief systems may always be in flux, and much information registers only as noise. Thus, images of televised eroticism may have little effect on many in the United States. Yet, the same images that almost are mundane in the United States could have dramatic effects if televised in China, Iraq, or Iran.[25]

Even though the democracy's social system may be fault-tolerant, its technomic control apparatus may be less so. Banking, finance, trade, travel, and air traffic control are now and increasingly will become more dependent on information technology systems. In 1992 the United States invested over $210 billion on information technology (about half the level of worldwide investment), and the amount invested is expected to grow about 18 percent each year for the next several years.[26] As dependence on information systems grows, warfare waged by nonstate groups_terrorists, religious extremists, hostile businesses_against information systems constitutes a real threat. The bombing of the World Trade Center, whatever other general or specific objectives it might have had, apparently was designed to inflict serious damage on the trading and banking capability of the United States. The information warfare component of some future strategic warfare campaign waged by terrorists certainly will not fail to include the power-production facilities and communications systems serving the principal target. Simultaneous attacks against widely dispersed nodes could have a strategic effect. That is, they could affect the knowledge, beliefs, and the will of leaders.

A cautionary note: because an information warfare campaign at the *strategic* level aims to subdue hostile will by affecting the knowledge and beliefs of the adversary, it cannot discriminate between combatants and noncombatants. Because the weapons of information warfare systematically attack the adversary's knowledge and belief systems (that which makes us different from other species), the likely outcomes of information warfare need to be evaluated consciously before information attacks are prosecuted. A successful information warfare campaign interposes a false reality on the human target. At the strategic level, these targets include both combatants and noncombatants. The interposition of a false reality ultimately may be as wrongful and inhumane as the wanton destruction of crops. To unhinge a noncombatant from reality, especially when the effects cannot be known or controlled, may be no less wrongful than to force another into starvation or cannibalism. Said another way, the principles of just war and just conduct in warfare need to be evaluated whenever *strategic* information warfare is contemplated.

Deception and disinformation, radio-electronic combat, propaganda, and the whole gamut of "psychological warfare" or command and control warfare attacks against enemy combatants at the *operational* level cannot be said to be wrongful. These aim to subdue without fighting or to reduce the amount of violence required. Becoming unhinged from reality in combat, like death or some other form of suffering, is a risk of which combatants are aware and is a possibility that combatants must accept. Thus, as long as information warfare and weapons are restricted by norms or laws to the operational level of warfare, it would appear that they are no more or any less evil than any other weapon. The problem remains a twofold one: determining the morality of an information warfare campaign waged at the strategic level and restricting the use of information weapons to the operational level.

The decision to pursue information warfare or develop information weapons is a leadership decision. It is a strategic decision in the United States because it is the Congress, representing the entire citizenry, that links means to ends. In the United States, such a program (if done by the state) would be done with money appropriated by the Congress. The Congress, or its oversight committees, will evaluate the morality of information warfare. In the wake of this evaluation, the Congress may confine these

weapons and their use to the operational level of warfare. The Congress may also establish safeguards to prevent any such weapons so developed from being used against internal constituencies. The legislative branch also may make laws preventing the use of information weapons against non-US noncombatants and internal constituencies. As out-sourcing and contracting-out initiatives increase, the Congress also can be expected to act to prevent some commercial enterprise from developing such weapons. (Have not news stories and "exposés" produced by commercial news enterprises proven to be contrived, aimed at influencing our knowledge and beliefs? Have not subliminal messages been used in the past in attempts to influence our purchasing behavior? Have not hackers entered and affected_or infected_databases already? We need to consider that there may be only a slim difference between a hacker and a terrorist in the information age. This is especially so if the hacker can attack things like finance, credit ratings, college transcripts, or other databases upon which technomic institutions depend.) The political leaders in the United States can be expected to consider the morality of information weapons and information warfare, no matter which group develops the weapons or engages in the warfare, and to regulate their use accordingly. The Congress very likely will conclude that the employment of information weapons at the operational level is useful and necessary, but that employment against noncombatants, or their employment at the strategic level is wrong.

The United States should expect that its information systems are vulnerable to attack. It should further expect that attacks, when they come, may come in advance of any formal declaration of hostile intent by an adversary state. When they come, the attacks will be prosecuted against both knowledge systems and belief systems, aimed at influencing leadership choices. The knowledge and beliefs of leaders will be attacked both directly and indirectly. Noncombatants, those upon whom leaders depend for support and action, will be targets. This is what we have to look forward to in 2020 or sooner.

Notes

1. Information warfare sometimes is erroneously referred to as command and control warfare, or C^2W. The aim of C^2W is to use physical and radio-electronic combat attacks against enemy information systems to separate enemy forces from enemy leadership. In theory, information warfare actually is a much larger set of activities aimed at the mind and will of the enemy.

2.Chris Mader, *Information Systems: Technology, Economics, Applications* (Chicago: Science Research Associates, Inc., 1974), 3.

3.The "waves" of societies are described by Alvin Toffler in *The Third Wave* (New York: William Morrow and Company, Inc., 1980). See also Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993). A seminal work on institutional forms is forthcoming from David Ronfeldt.

4.John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 2 (April-June 1993): 141-65.

5.Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991), 196-205. Words like *war* and the lately contrived *warfighter* confuse the *warriors* in a democracy by misuse. In the United States, *War* (with a big *W*) is declared by the Congress: the people representing all the people. Executive *War Powers* are really *warfare powers*. The days of Clausewitzian, trinitarian *W*ars may very well be over, as van Creveld suggests. The days of warfare, however, are not over.

6.Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 77.

7. Richard Szafranski, "Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill," *Military Review*, November 1994; and idem, "When Waves Collide: Conflict in the Next Century," *JFQ: Joint Force Quarterly*, Winter 1994-95.

8.Joseph A. Engelbrecht, "War Termination: Why Does a State Decide to Stop Fighting?" (PhD diss., Columbia University, 1992). Colonel Engelbrecht is a colleague at the Air University's Air War College.

9.Arquilla and Ronfeldt, note 9, 162. According to this definition, a message with no discernible "meaning" is still "information." This definition is useful when contemplating the tactics of information warfare.

10.Ibid.

11.*Phenomenology* can be defined as "the theory of the appearances fundamental to all empirical knowledge." Dorion Cairns, in Dagobert D. Runes, ed., *Dictionary of Philosophy* (Totowa, N.J.: Littlefield, Adams & Co., Ltd., 1962), 231-34.

12. C. G. Jung, *The Undiscovered Self* (New York: The New American Library, Mentor Book, 1958), 102.

13.Information warfare requires that philosophers, cultural anthropologists, area specialists, linguists, and semanticists join the "operations" staff. The days have passed when war colleges or staff colleges could neglect these other disciplines.

14.John R. Boyd, briefing slides, subject: A Discourse On Winning and Losing, August 1987. Maxwell AFB, Alabama.

15.Ibid.

16.Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), book 6, chapter 6, 372-76.

17.Ledger Wood, in Runes, 94-96.

18.The effects to which I refer are more complicated than the inability to prevent your own jamming from interfering with your own communications systems. These unconfinable, spillover effects of stray electrons can be modeled and some compensation can be made for their effects. The weapons and effects of information warfare are not so easily confinable or controllable. In warfare it is common to both demonize and ridicule the enemy. Ridicule often takes the form of jokes. If these jokes ridicule an enemy from a different ethnic group, these jokes become officially sanctioned racist jokes. If the ethnic group is part of our own citizenry, such attacks can cause collateral damage. The collateral damage to the armed forces may have effects as far-reaching as the appearance of officially condoned racism. If one accepts that weapons and attacks have stochastic effects, then some consequences are unpredictable.

19.Van Creveld, 35.

20.*Grant T. Hammond, "Paradoxes of War," JFQ: Joint Forces Quarterly*, Spring 1994. Dr Hammond is a colleague on Air University's Air War College faculty.

21.George C. Kohn, *Dictionary of Wars* (New York: Facts On File Publications, 1986), 214.

22.*Technomic* is a word coined by Col Joseph A. Engelbrecht. He defines it to mean "of or relating to progress in the development of the application of scientific principle (technology), and in the development of wealth (economics), and in the interrelationship between advances in science and the spread and increase of economic wealth. Technomic vitality. Technomic proliferation."
23.Gerald R. Hurst, "Taking down Telecommunications" (Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Ala., 28 May 1993).

24.Ibid.

25.Iran provides a good example. The Majles investigation into the Iranian department of "Voice and Vision" illuminates Iran's sensitivity to the content and meaning of pictorial messages. Consider these comments from the investigation:
A basic criticism of the pictorial programs of the Voice and Vision is lack of attention to full veiling of women, lack of attention to the chador, and spreading of the culture of the "manteau" and scarves of the immoral kind.
The grand leader on occasions has given opinions and directives to the Voice and Vision organization or its director. Unfortunately, the instructions and directives of his honor were not implemented. For example: . . . . From 1368 [21 March 1989-20 March 1990] to 1370 [21 March 1990-20 March 1991], he made reminders to the Voice and Vision on 14 occasions, the most important of which concern: A) Misinformation. B) The low level of quality of the beyond-the-border programs and failure to propagate and spread Islamic views in them. C) The broadcast of blasphemous sentences concerning the Sire of the Pious. . . . E) Showing actual persons in the role of the infallible imams.
See "Majles Investigates Activities of Voice and Vision," 3, 4, 15 November 1993, 5-6, in *Foreign Broadcast Information Service Report: Near East and South Asia* (FBIS-NES-94-016-S), 25 January 1994, 6-8. I am grateful to Dr George Stein of the Air University's Air War College faculty for pointing out this example of what simultaneously might be internal information warfare and potential vulnerability to external information warfare. Saudi Arabia recently joined China as the most recent nation to outlaw satellite television receivers. One can easily appreciate the effects that Music Television (MTV) might have on such cultures.

26.A telecommunications executive speaking in an Air University forum under the promise of nonattribution disclosed these estimated figures.