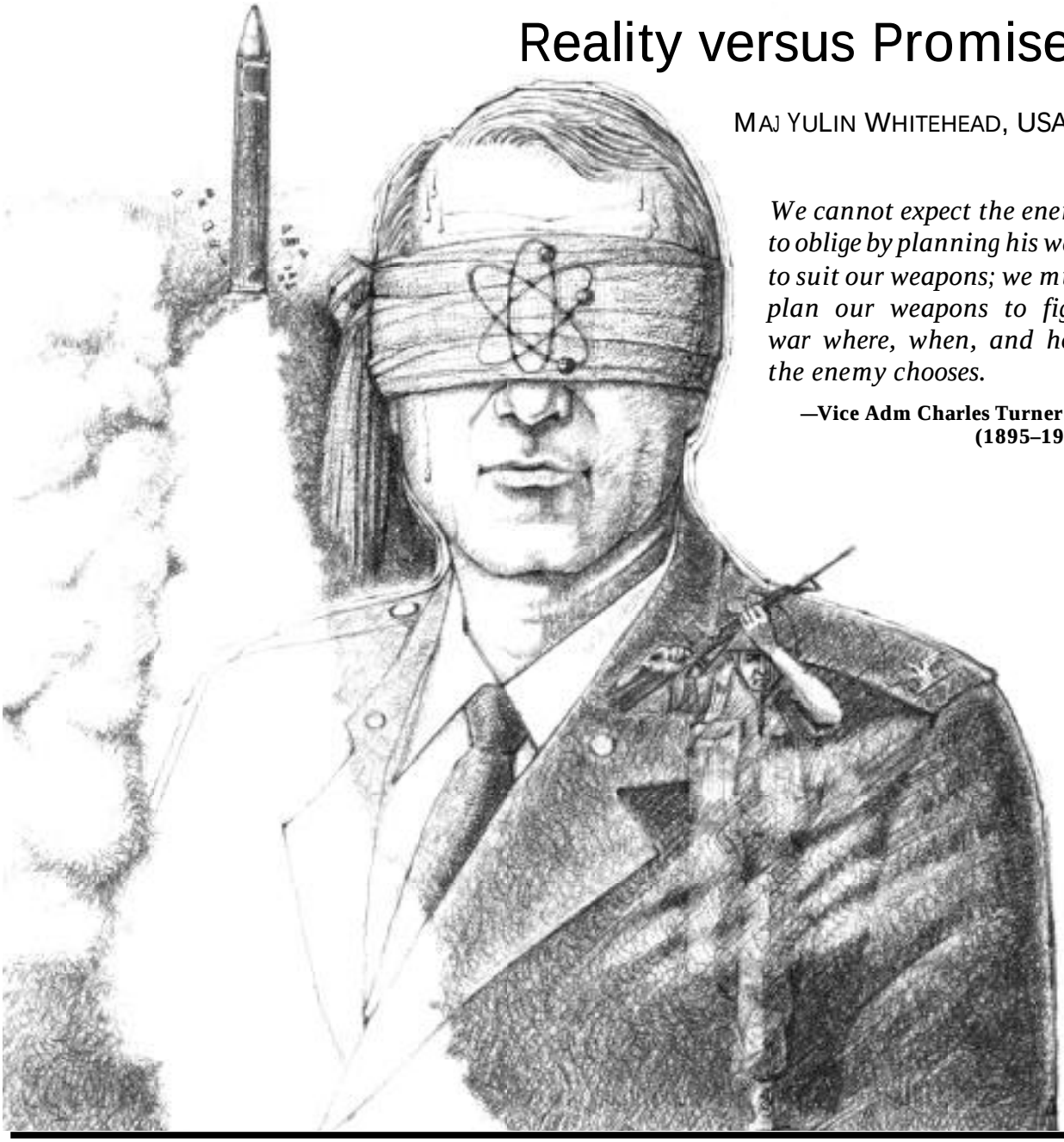
Information as a Weapon

Reality versus Promises

MAJ YULIN WHITEHEAD, USAF*



We cannot expect the enemy to oblige by planning his wars to suit our weapons; we must plan our weapons to fight war where, when, and how the enemy chooses.

—Vice Adm Charles Turner Joy (1895–1956)

The instruments of battle are valuable only if one knows how to use them.

—Ardant du Picq, *Battle Studies*

THERE ARE MANY views of what constitutes information warfare (IW). The differences in interpretation are understandable given the subtle (and sometimes not-so-subtle) variations in the defi-nitions of IW. Also, the various terms used a s sub sti tu tions for IW add to the differing views of the topic. The differences in interpre-tation have translated into a virtual explosion of literature written by authors with their own definitions of IW.

The literature may be grouped into two broad categories based on the authors' thematic approach to IW. The first category involves a con cept that dis cusses IW in terms of the more traditional notion of the use of "information warfare" to support decision making and combat operations. This first theme does not address the question of whether information is a weapon and is there-fore inappropriate for this article. On the other hand, the second category is a wholly different approach and one that directly pro-vides evidence to support or refute the ques-tion of whether information is a weapon. Authors in this category regard "information as a weapon" in warfare.

Dr. George J. Stein, a professor at the US Air Force's Air War College, also sees a clear separation between using "information in warfare" and using "information as a weapon" or what he terms *information warfare* or *information attack*.[1] He believes that there is significant differ-ence be tween the two cate go ries. Spe cifically, he explains information in warfare as

> all those papers and briefings that begin "Information has always been central to warfare . . ." and then go on to explain that "our new computer system will get information to the warfighter" so he can "achieve information dominance on the battlefield" and thus demonstrate our service's mastery of IW, confuse information-in-war with information warfare. Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW.[2]

The US Air Force document *Cornerstones of Information Warfare* makes a similar distinction by dis tin guish ing the dif fer ence be tween *information age warfare* and *information warfare*. It explains the former as "us[ing] information technology as a tool to impart our com bat operations with unprecedented economies of time and force,"[3] such as cruise missiles exploiting in for ma tion age tech nologies to put a bomb on target. Information war fare, how ever, "views in for ma tion it self as a separate realm, potent weapon, and lucrative target"[4] and fits in the category of using information as a weapon.

Using this typology, it appears many of those who claimed Operation Desert Storm was an in for ma tion war are ac tu ally de scribing the use of information in warfare or information age warfare.[5] For example, Alan D. Campen, a former undersecretary of defense for policy, states that "this war dif-fered fundamentally from any previous conflict [and] the outcome turned as much on superior management of *knowledge* as it did upon performances of people or weapons."[6] Further, us ing this defi ni tion, he and others argue that Operation Desert Storm was not only an information war, but the first one in history. This ar gu ment holds lit-tle credibility because it was not the first time an armed force failed to attain victory for lack of knowledge.[7]

The USAF and Dr. Ste in's cate go ri za tions of the use of "in for ma tion as a weapon" and "information in warfare" provide a logical method to separate the two main themes of information warfare literature. However, it is not the author's intent to argue the merits or faults of their de line a tions. Rather, this ar ti cle

*Special thanks to Dr. Daniel J. Hughes, professor of military history, Air War College, and Maj Mark J. Conversino, professor of airpower history and theory, School of Advanced Airpower Studies, for their invaluable advice and guidance in the writing of this article. Also, thanks to my husband, Ray, for his constant love and support.

During Desert Storm, Lt Gen Frederick Franks, VII Corps commander, sketches his plan to envelop remaining Iraqi forces. Instead of just contemplating whether the information weapon will affect an enemy's will to fight, one should ask how US military leaders would react if an adversary blinded friendly command and control systems.

uses those writings that profess the use of information as a weapon rather than those that boast the effective use of information in warfare in supporting combat operations, since the latter is not relevant to the question of whether information is a weapon.

The Information Weapon

Identifying literature that advocates information as a weapon is fairly elementary. The authors usually declare their beliefs with such definitive statements as "The electron is the ultimate precision guided weapon";[8] "Information is both the target and the weapon";[9] "The day may well come when more soldiers carry computers than carry guns";[10] "The US may soon wage war by mouse, keyboard and computer virus";[11] "Information may be the most fearsome weapon on the emerging techno-battlefield";[12] "The most potent new US weapon, however, is not a bomb, but a ganglion of electronic ones and zeroes";[13] and "In Information Warfare, Information Age weaponry will replace bombs and bullets."[14] Certainly this is not a comprehensive list of information warfare–related writings that proclaim information as a weapon, but it does represent a cross section of ideas that appear in publications that range from official government documents to more popular books and magazines meant to attract the average reader.

After one gets past the attention-getting steps of pithy statements proclaiming information as a weapon and a target, one signifi-

cant theme emerges. Specifically, the "information weapon" advocates believe "information warfare can enhance power projection by diminishing an adversary's will and capacity to make war."[15] Linking the information weapon to the enemy's warfighting capabilities and will to fight is significant because US military thinking has evolved to accept that diminishing these two aspects of an opponent will lead to victory for our own forces.[16] The US Army field manual on information warfare explains the significance of this linkage by equating the information weapon to the purpose of firepower in combat—"the generation of destructive force against an enemy's capabilities and will to fight."[17]

Similarly, literature not under the purview of the Department of Defense (DOD) also expounds on the ability of the information weapon to affect the enemy's ability and will to fight. The most apparent difference between official DOD publications and popular literature is that the latter may not employ the exact phrase of using information to affect "the adversary's will and capacity to make war." Nevertheless, this is a firmly established concept that appears frequently in writings about information warfare. For example, Col Richard Szafranski, USAF, Retired, a former Air War College professor who has written extensively on various military-related topics, equates subduing the enemy's will to "neocortical warfare," which "strives to influence, even to the point of regulating the consciousness, perceptions, and will of the adversary's leadership: the enemy's neocortical system."[18]

Other advocates of the information weapon either do not specifically address what constitutes a "target" or tend to agree in principle with the Air Force definition. While the latter group of advocates agrees that the target is information, their description of the "information target" may be more esoteric. As a case in point, Stein explains that "information attack, while 'platform-based' in the physical universe of matter and energy, is not the only counter-platform," and he believes that doctrinal thinking must move away from the "idea that information attack involves only the use of computers and communications."[19] He incorporates John Boyd's "observation-orientation-decide-act" (OODA) loop[20] in defining the targets of the information weapon. Stein sees indirect information warfare attacks as affecting the "observation" level of the OODA loop at which information must be perceived to be acted on.[21] On the other hand, direct information warfare corrupts the "orientation" level of the OODA loop to affect adversary analysis that ultimately results in decision and action.[22] Thus, to him, the information weapon may or may not be used against a counter platform. Stein's bottom line is that "information is both the target and the weapon: the weapon effect is predictable error."[23] The weapons effect of "predictable error" resulting from the use of the information weapon is an incredible notion because it assumes that one can predictably induce errors an adversary will make in "observing" and "orienting" information that ultimately results in decision and action.

In another example, Szafranski, in the most general terms, appears to agree that the information weapon affects the information target but wants his readers to focus on the "enemy mind" as a whole. He states that

> 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." 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.[24]

In Szafranski's construct, the "acme of skill" is to employ the information weapon to "cause the enemy to choose not to fight by exercising reflexive influence, almost parasympathetic control, over products of the adversary's neocortex."[25]

Thus, the prototypical advocate of using information as weapons espouses the aim of such weapons as to influence an adversary's will and capacity to make war. Further, with information as the weapon, its target, in the

simplest sense, is also information. A more esoteric definition of the target is the enemy mind or his cognitive and technical abilities to use information. Finally, the explicitly stated and sometimes implicitly assumed weapons effect is predictable error. Specifically, the use of the information weapon will allow one to predict how an enemy will err in judgment, decisions, and actions.

Enemy Will and Capacity to Fight

There is a paucity of evidence available for analysis in addressing the information weapon's effect on the "adversary's will and capacity to fight." Most of the literature tends to identify either "information" or the "enemy mind's ability to observe and orient" as the targets of the information weapon. Unfortunately, these two concepts can either encompass every target or are so esoteric that it is difficult to identify specific targets. The remainder of this portion of the analysis will first address the "information" target and then tackle the target of the "enemy mind's ability to observe and orient."

It appears that the US Air Force has recognized the difficulty of identifying specific information targets and has attempted to address the issue through its *Cornerstones of Information Warfare* pamphlet and draft doctrinal documents. For example, the Air Force has stated, "Information warfare is any attack against an information function, regardless of the means."[26] Therefore, "bombing a telephone switching facility is information warfare. So is destroying the switching facility's software."[27] Similar types of targets may then include elements of the enemy integrated air defense system (IADS). In defining the information target, the US Air Force is attempting to focus information warfare as "a means, not an end, in precisely the same manner that air warfare is a means, not an end."[28] However, an unintended consequence may result from this overarching target definition: if information warfare encompasses nearly every target, then the concept merely becomes a new label for traditional military operations (such as psychological operations, deception, physical destruction, etc.) that military forces have conducted for thousands of years.

Do the information weapon attacks against communications and control facilities, the enemy's IADS, and their computers diminish the adversary's will and capacity to fight? Well, yes and no. Certainly, "hard killing" elements of the enemy information functions or "soft killing" through introduction of viruses and logic bombs into the enemy's computer systems would affect his capacity to fight. Hard kills result in the physical destruction of information systems and interconnections, while soft kills render computer screens "blank" or cause the systems to present faulty displays.

Given that the information weapon could affect an enemy's capability to fight, will it also be able to affect his will to fight? While the enemy computer terminal operator may feel frustrations and even decreased morale resulting from leaders' demands for unavailable information, the latter's will to fight may or may not be affected. In other words, how would "blinding" enemy leaders affect their will to fight? Would they actually surrender, or would US blinding operations actually backfire and force adversary leaders to panic and resort to the use of weapons of mass destruction? For example, Russia adopted a military doctrine in November 1993 that indicated a belief that during an East-West conflict, an attack on Russia's early-warning system for strategic nuclear forces is possible.[29] In such a situation, the Russians may assume the worst—the invasion of Russian territory by foreign military forces. With their sensors blinded and command and control systems destroyed by information weapons, Russian leaders may not be able to obtain information and may resort to whatever means necessary to protect their homeland. In essence, they will be "blind," but their strategic nuclear weapons will still be intact and operable. How can the information weapon advocate be certain that Russia will not employ the nuclear weapons?

The Scud problem during Desert Storm demonstrated that coalition efforts to blind and paralyze the enemy, while impressive and important, did not in themselves diminish the capability or will of the Iraqis to fight.

Instead of just contemplating whether the information weapon will affect an enemy's will to fight, one should ask how US military leaders would react if an adversary blinded friendly command and control systems. Would US military leaders lose the will to fight if their computers went blank? The will to fight is an elusive target, and it is difficult to assess whether the information weapon is capable of affecting it. Certainly, other factors such as political objectives and the question of whether the enemy is fighting for his own survival or for more limited goals would surely figure into the will-to-fight equation.

Despite the value of "will," some information weapon advocates, drawing from Col John Warden's view of the enemy as a system, argue that the relationship of will (morale) and the capacity to fight (physical) can be expressed in the following equation:[30]

(Physical) x (Morale) = Outcome

Specifically, they believe that a weapon need not affect both will and capacity to fight to put the enemy in such a condition that he can no longer carry on the fight. In fact, Colonel Warden states that the physical part of the equation is easier to target than morale, so US forces should focus on the physical. He asserts, "If the physical side of the equation can be driven close to zero, the best morale in the world is not going to produce a high number on the outcome side of the equation."[31] Clausewitz cautioned against this type of reductionism and wrote, "If the theory of war did no more than remind us of these elements, demonstrating the need to reckon with and give full value to moral qualities, it would expand its horizon, and simply by establishing this point of view would condemn in advance anyone who sought to base an analysis on material factors alone."[32]

Indeed, numerous historical cases support Clausewitz's warning of not underestimating the importance of morale or the will to fight. One of the most distinct examples for the United States remains the Vietnam War during the 1960s and early 1970s. Despite the US military's efforts in destroying the Vietnamese communists' material resources and sig-

nificantly reducing the movement of their lines of communication along the Ho Chi Minh Trail, the communists retained their will to fight.[33] In the end, it was their tremendous will to fight and, arguably, the US lack of will to fight that allowed North Vietnam to defeat the United States and the Saigon regime.[34]

Nevertheless, advocates of the information weapon's effectiveness use the "information warfare" actions in Operation Desert Storm to show that destruction of the capacity to fight (physical) affected the will to fight (morale):

> Coalition forces spent the early days of Desert Storm gouging out the eyes of Iraq, knocking out telephone exchanges, microwave relay towers, fiber optic nodes and bridges carrying coaxial communications cables. By striking Hussein's military command centers, the coalition severed communications between Iraqi military leaders and their troops. With their picture of the battlefield—their battlefield awareness—shrouded in a fog, the Iraqis were paralyzed.[35]

Noticeably lacking from this illustration is the explanation that after the supposed "paralysis" of the Iraqis, deployed coalition military forces fought an air and ground war in Iraq. The combination of coalition air forces that bombed Iraqi targets from 17 January to 2 March 1991 coupled with the coalition ground attack that began on 24 February 1991[36] ultimately led to Iraq's agreement to accept all terms of the United Nations cease-fire resolution.[37] In other words, the efforts to blind and paralyze the Iraqis, while impressive and important, did not by themselves diminish their capability or will to fight. Rather, the blinding efforts made the Iraqis more vulnerable to conventional coalition military attacks and operations.

The Operation Desert Storm illustration, besides being a reductionist argument that distorted the nature and causes of US and coalition military successes against the Iraqi forces, also ignored other realities. First, several Desert Storm analysts suspected that after coalition forces destroyed Saddam Hussein's more advanced telecommunications systems (satellite, microwave, and cable systems), he continued to relay launch orders to his Scud missile batteries via courier.[38] Second, the often simplistic method depicted regarding the ease with which the United States took down the Iraqi command network may have been overstated.[39] Specifically, while coalition airpower greatly reduced the capacity of the communication links between Baghdad and its field army in the Kuwaiti theater of operations, sufficient connectivity remained for Baghdad to order a withdrawal from Kuwait that included some redeployments to screen the retreat. Therefore, the ambitious hope that bombing the leadership and command, control, and communications targets would lead to the overthrow of the Iraqi regime and completely sever communications between the Baghdad leadership and their military forces "clearly fell short."[40] Third, the Iraqi forces, the Republican Guards notwithstanding, were poorly trained and motivated, and lacked high morale prior to any coalition information attack. Thus, it was not the effect of the information weapon alone that weakened the enemy's will to fight.

There are other examples of military forces that continued to fight after being isolated from higher headquarters when their communications became inoperable. During the Normandy campaign in 1944, German forces often fought under emissions control or radio silence. Yet, their effective training, sound tactical leadership and doctrine, and adherence to *Auftragstaktik*, or mission-type orders, enabled them, for almost two months, to fight the numerically superior Allies to a stalemate before attrition finally wore down their effectiveness.[41]

Perhaps those who advocate using the information weapon against the second type of information target, the "enemy mind's ability to observe and orient," place more importance on the morale factor than the physical. Champions of attacking this type of information target have coined this form of information warfare as "perception management,"[42] "orientation management,"[43] or "neocortical warfare."[44] While these terms may imply some "new" types of warfare, in actuality they are

merely amorphous terms for what had been traditionally called psychological operations, propaganda, and military deception. For the purpose of discussion, this article addresses this form of information weapon as perception management.

The same question posed about information as a target also applies to the second information target, the enemy mind. The key question is whether information warfare will necessarily reduce the mental ability and will to resist. While it is true that perception management can deceive, surprise, add to the enemy's fog and friction, and even affect the morale or the will to fight, it will not likely produce a "predictable error" as Dr. Stein assumes.[45] The concept of producing a "predictable error" implies that one can predictably induce advantageous errors in an adversary's actions and decision making. In essence, it assumes that human behavior and reactions are totally predictable and may be precisely manipulated. This concept ignores Clausewitz's philosophy of the unpredictability of humans and warfare as illustrated through the following syllogism:

If A ≠ B (If humans do not behave according to laws)
And C = A (And warfare is a human event)
Therefore, C ≠ B (Therefore, warfare will not follow laws)

Not only does the concept of "predictable error" ignore Clausewitz's theory regarding human nature and warfare, it also seems to challenge common sense. For example, is it really possible to predict the actions, intent, and decision-making rationale of such disparate minds as those of Adolf Hitler, Joseph Stalin, Ho Chi Minh, Ayatollah Ruhollah Khomeini, Mu'ammar Gadhafi, Saddam Hussein, Mohammed Aidid, and Kim Jong Il? Hitler thought he could achieve a predictable outcome when he drew up the Operation Barbarossa plan and "believed nothing less than the Soviet Union could be defeated in four months."[46] Yet, in April 1945, Soviet tanks entered Berlin, almost four years after German forces invaded the Soviet Union in May 1941. A "predictable error" may be extremely difficult to predict, much less to induce.

In the same vein, perception management will likely have minimal impact on the enemy's capacity to fight, unless, of course, the "information attack" deceives the enemy regarding the disposition and location of friendly forces. As an illustration, the World War II Allied deception plan, Operation Fortitude, contributed to Adolf Hitler's preconceptions of the location of the impending invasion of France. Consequently, invading Allied forces at Normandy did not face the bulk of the German troops in France and Belgium guarding the Pas de Calais and the Belgian and Dutch coastline.[47]

Somewhat more troublesome is the view of many of these advocates who believe it is possible to use the perception management weapon to target the enemy mind with "the aim of subduing hostile will without fighting."[48] They balk at the view that this type of attack should supplement and enhance more conventional forms of warfare. Again, the literature is sparse in terms of specifics on how perception management will "subdue hostile will." But it does not lack in promises to stop a war before it starts. One example of how this type of attack might target hostile will was posed by Thomas Czerwinski, a professor in the School of Information Warfare and Strategy at the National Defense University. "What would happen if you took Saddam Hussein's image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?" While it is not possible to state with absolute certainty the reactions of the Baath Party, Saddam Hussein, or the world community, it is unlikely that such perception management attacks will completely subdue hostile enemy will. Those who predict it is possible to subdue enemy will with perception management seem to assume, as in this example, that enemy leaders will have no interactions with their followers.

Civilian and military leaders have used perception management, or propaganda, throughout the history of warfare. The difference today is brought about by the advent of the microprocessor, which al-

lows another medium, cyberspace, for friendly forces to propagate the perception management message to the enemy. Unfortunately, propaganda has had, at best, limited utility. To elevate its stature above that of a supplemental role in war is unrealistic.

It is inconceivable to expect perception management alone to subdue a hostile's will to fight, especially when history has shown otherwise. The idea that perception management will enshroud the enemy in "fog" and "friction" and subsequently subdue his morale assumes the enemy will react exactly as the propaganda plan expects. This assumption discounts historical cases. For example, during World War II, the US military, having nearly destroyed Japan's capacity to fight, targeted the will of the people through leaflet drops and firebombings of cities with populations over one hundred thousand, along with the release of two atomic weapons on Hiroshima and Nagasaki. Despite the horrific death and destruction, Japanese military commanders refused to surrender, and the Japanese people were in despair after hearing of their emperor's decree to surrender.[49] How realistic, then, is the information weapon advocates' vision that enemies will surrender through information attacks targeted at the enemy mind or "neocortical" system? Will the enemy stop fighting because the United States, through perception management attacks, tells him to stop? Unfortunately, the enemy may not always be so cooperative.

The results of a blinded and paralyzed Iraqi military. Scuds were being launched throughout the war.

The Information Weapon: Use with Caution

In analyzing whether information is a weapon, this article tested the ability of information itself to target "information" and the "enemy mind's ability to observe and orient" for the purpose of destroying the enemy's will and capacity to fight. The results indicated that while information may be considered a weapon, it is one that must be used with caution. The more enthusiastic proponents of the information weapon tend to overestimate its ability to diminish enemy capacity and will to fight.

Information is not a technological "silver bullet," able to subdue the enemy without battle. Unlike other, more conventional, weapons, the effects of the information weapon are not necessarily predictable because it often targets the human mind and emotions. Thus, in employing the information weapon, one must not rely solely on its use for success. Rather, the strategist must prudently use the information weapon to supplement more traditional weapons of war or as a precursor to conventional attacks and operations.

While this article has answered the question it set out to investigate, other factors have emerged in the course of this analysis. The extreme claims for information warfare, even when employing the information weapon as envisioned by its advocates, are particularly unconvincing and even irresponsible. The most zealous advocates of information warfare describe information as a low-cost weapon with a high payoff, a method to eliminate the fog and friction of war for friendly forces yet enshroud the enemy in the same, and a tool to allow attainment of quick and bloodless victories.

Regarding the first characteristic, a low-cost weapon with a high payoff, the cost will depend on the specific information weapon itself. Certainly, introducing a virus or logic bomb into a computer system may be a relatively low-cost option, whereas physical destruction of the enemy IADS will likely accrue significant costs. The claim of a high payoff is also debatable. As previously discussed, "predictable errors" may be extremely difficult to predict and induce as the information weapon often targets human reactions and emotions.

In an ideal world, fog and friction would be eliminated for friendly forces and yet maximized against the enemy. However, the exact information weapons intended to increase the enemy's "fog of uncertainty" may lead to totally unintended consequences that are inconsistent with the original intent of the weapon. Worse, the nth-order effect may actually prove counterproductive to the original intent and objective. In a complex, hierarchical command and control system, destruction of selected communications connectivity may actually result in a more streamlined and efficient command and control system. At least three unintended consequences may result. First, the enemy leader, without the intermediate command and control steps, is now able to send his orders directly to the lower echelons. For example, during Operation Desert Storm, after coalition forces destroyed Saddam Hussein's more advanced telecommunications capabilities, he continued to relay launch orders to his Scud missile batteries via courier.[50] Second, if communications connectivity is severed, lower echelons will likely operate in autonomous modes. While they may lack the complete situational battlefield picture that upper echelons would normally provide, the lower echelons benefit by not having to wait for launch orders to flow from the top. Third, destroying or degrading enemy command and control systems may deny friendly forces the ability to collect vital enemy communications and signals. Thus, employment of the information weapon may actually simplify enemy operations and increase friendly fog and friction, since friendly collection assets will not be able to collect against emitting enemy electronic systems.

Perhaps the most disturbing claim is that of the information weapon's capability to attain quick and bloodless victories and its extreme view of preventing a war before it starts.

While the information weapon may be able to prevent bloodshed in a limited number of scenarios, expecting it to end a war before the first shot is fired is pure speculation. A more realistic consequence resulting from the employment of the information weapon would be a degraded enemy that lacks complete battlefield situational awareness because leaders are blinded and cannot communicate with troops in the field. There is a lack of historical evidence that supports the concept that a blinded enemy would simply surrender without fighting. On the contrary, history shows military forces, isolated from higher headquarters, do continue to fight. As previously mentioned, the German military, during World War II, emphasized *Auftragstaktik*, which relied on general guidance from above combined with lower echelon initiative.[51] This philosophy resulted in German forces fighting under radio silence, without upper echelon guidance, as during the Allied Normandy campaign.

Maj Gen Michael V. Hayden, commander of the Air Intelligence Agency, summed it best when he called the "notion of a bloodless war played out on computers as fanciful" and said that he does not foresee the United States mothballing its stockpile of conventional and nuclear weapons in the near future. Further, he stated, "Can I imagine a time in which we won't have destructive war? No. But I think it's easy to imagine a time when we can use information as an alternative to traditional warfare." General Hayden relayed the following incident to describe the use of the information weapon to help create the zone of separation between warring factions in Bosnia:

> Some of the factions didn't comply completely. But the Implementation Force goaded, forced, cajoled and pressured them to do it. One of the things they did was take clear evidence [and] information that they had not complied with the treaty. The IFOR commander turned to the Serb, the Croat and the Muslim and said, "Move those tanks." Their response was "What tanks?" The commander says, "These tanks," pointing to the concrete evidence. "Oh, those tanks," they said. And then the tanks were moved. In Bosnia, I think it's fair to say, information is the weapon of first resort. To back that up is the potential for heat, blast and fragmentation. But in this case, information was used as an alternative. We achieved an objective without going immediately to some sort of destructive approach.[52]

It is clear that while information may be used as a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to blind the enemy prior to conventional attacks and operations.

The US military arsenal includes a variety of weapons, and the strategist must ensure their most effective use in future wars. The strategy of the future will likely include the use of the information weapon in conjunction with more conventional weapons. In developing the plan, the strategist must realize that the use of the information weapon will demand prudence and carry implications that may impact the employment of the weapon. The last section warns of the additional cautions that a strategist planning to employ the information weapon must consider.

Implications

One characteristic of the US military and its way of war is its fascination with technology and the associated search for the high-tech silver bullet that will allow quick victories with minimal collateral damage.[53] Hence, it is not surprising that extremists have embraced information warfare as the magic weapon that would allow the US military to win bloodless victories and end wars before the first bullet is ever fired. The use of the information weapon demands caution, and its employment carries with it implications that the strategists must consider.

First, perhaps one reason for the vast interest in the application of information warfare is that the United States may be the most vulnerable to its effects. As Lt Gen Kenneth A.

During Desert Storm, the blinding efforts made the Iraqis more vulnerable to conventional coalition military attacks and operations. A destroyed Iraqi helicopter and its shelter (above) and damaged Iraqi equipment at a Euphrates River crossing (below).

Minihan, director of the National Security Agency, explained, "Information is both the greatest advantage and, given American dependency on information, the greatest weakness of the US."[54] Consider the following assertion: "Under IW, the enemy soldier no longer constitutes a major target. IW will focus on preventing the enemy soldier from talking to his commander. Without coordinated action, an enemy force becomes an unwieldy mob, and a battle devolves to a crowd-control issue."[55] Is this actually an analysis of the vulnerability of our own US military to information warfare? Given the US system of assigning specific targets to individual aircraft via the air tasking order (ATO), the descriptions of enemy vulnerability to the information weapon may actually be a reflection on the American air campaign process. Could an information weapon bring the air operations center (AOC) to a standstill if it destroyed computers within the AOC, leaving it with no capability to develop and transmit the ATO to flying wings?

A second implication concerns the importance of maintaining US combat readiness with conventional military forces. Eliot Cohen, noted author and professor at Johns Hopkins University, warned, "Transformation in one area of military affairs does not, however, mean the irrelevance of all others. Just as nuclear weapons did not render conventional power obsolete, this revolution will not render guerrilla tactics, terrorism, or WMD [weapons of mass destruction] obsolete."[56] The US military must, therefore, remain capable of fighting less technologically advanced enemies as well as peer competitors. History is full of examples of less technically developed militaries overcoming and defeating more "capable" foes. The most vivid example for the United States remains the Vietcong, who were able to defeat technology with rudimentary tactics and a willingness to sacrifice their soldiers. In facing a Vietcong-type adversary, can the United States realistically expect to defeat an enemy without resort to heavy destruction, or at least having in place the potential to do such destruction?[57]

A third implication that civilian and military leaders must seriously consider is the legality of information warfare. This question is especially important when one considers "preemptive" information attacks. One envisioned characteristic of information warfare regards the use of the information weapon to end a war before the first shot is fired. How will the international community react to this type of preemptive attack by the United States, a superpower, especially if it is against a third world rogue power? Is the United States willing to risk an information attack that would blind a peer competitor and risk escalating the conflict with the use of weapons of mass destruction? Is an information attack an act of war? Further, the use of perception management, especially one that alters an enemy leader's image to tell his people to surrender, is comparable to faking surrender with the use of the traditional white flag. This and other actions may violate the "principle of chivalry which addresses the use of trickery," both permissible ruses and impermissible perfidy and treachery."[58]

Obviously, the potential consequences of the employment of the information weapon are new and evolving, and the implications of information warfare raise many issues that have no clear legal precedent.[59]

Conclusion

The information weapon may be an effective tool to supplement the military's arsenal of more traditional weapons. Further, its use as a precursor may enhance conventional attacks and operations against a blinded and degraded enemy, thus decreasing effective enemy defense and counterattacks. However, the United States should not consider the information weapon a "silver bullet" that will completely subdue an adversary's will and capacity to fight. Further, strategists must refrain from uncritically assuming the information weapon is capable of terminating wars before the first bullet is even fired.

The US civilian and military leaders should strive to understand why information warfare appears so attractive, in order that realistic and useful doctrinal guidance may be developed for its employment and incorporation into the overall war-fighting strategy. The consequences of not accomplishing this self-examination could result in the military promising too much, too fast. □

Notes

1. Dr. George J. Stein, director, International Security Studies core and professor of European Studies at the US Air Force Air War College, Maxwell AFB, Ala., interviewed by author, 9 October 1996. Dr. Stein's interest in information warfare began with his participation in the Air Force chief of staff–directed SPACECAST 2020 study at Air University, Maxwell AFB, Ala., in academic year 1994/1995.

2. Dr. George J. Stein, "Information Attack: Information Warfare in 2025," in *2025 White Papers: Power and Influence,* vol. 3, bk. 1 (Maxwell AFB, Ala.: Air University Press, November 1996), 98.

3. USAF, *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force, 1995), 2.

4. Ibid.

5. Soon after Operation Desert Storm, several noted authors claimed that Operation Desert Storm was the "first information war." They include Alan D. Campen, ed., *The First Information War* (Fairfax, Va.: AFCEA International Press, October 1992); and Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown & Co., 1993).

6. Campen, vii. Other examples include Toffler and Toffler, 69. The Tofflers stated that the Gulf War represented a completely "new form of warfare." They asserted that "a revolution is occurring that places knowledge, in various forms, at the core of military power." Three RAND defense analysts asserted that "Desert Storm represented the first modern 'information war,' in that every aspect of military operations depended to some degree on information provided by many systems operating in various media and at all echelons." James A. Winnefeld, Preston Niblack, and Dana J. Johnson, *A League of Airmen: US Airpower in the Gulf War* (Santa Monica, Calif.: RAND, 1994), 182 and 219.

7. Col Edward C. Mann III, *Thunder and Lightning: Desert Storm and the Airpower Debates* (Maxwell AFB, Ala.: Air University Press, April 1995), 146. Colonel Mann directly challenged Alan Campen's claim that Operation Desert Storm was the "first information war" by pointing out that "Campen tacitly avers the truth—suggested by Sun Tzu 2,500 years ago—that the ultimate goal of the struggle is to dominate the enemy in knowledge—not information. Collection and analysis of information is, of course, a part—but not the whole—of the issue."

8. Quoted in John T. Correll, "Warfare in the Information Age" (editorial), *Air Force Magazine* 79, no. 12 (December 1996): 3. John M. Deutch, former director of Central Intelligence (DCI), testified on 25 June 1996 before the US Senate Committee on Government Affairs on the subject of "Foreign Information Warfare Programs and Capabilities." Deutch had served dual-hatted roles as both the DCI and director, Central Intelligence Agency (CIA). The National Security Act of 1947 designates the DCI as the primary adviser on national foreign intelligence to the president and the National Security Council. The DCI is tasked with directing and conducting all national foreign intelligence and counterintelligence activities. To discharge these duties, the DCI serves both as head of the CIA and of the US Intelligence community. It was in his DCI capacity that Deutch testified before the US Senate. In discussions regarding offensive information warfare capabilities, Deutch told Congress that "the electron is the ultimate precision guided weapon." His opening remarks during this testimony are on-line, Internet, 17 March 1997, available from http://www.odci.gov/cia/public_affairs/speeches/dci_testimony_062596.ht ml.

9. *Cornerstones of Information Warfare,* 2–3; and Stein, "Information Attack," 105.

10. Toffler and Toffler, 71.

11. Douglas Waller Washington, "Onward Cyber Soldiers," *Time,* 21 August 1995, n.p.; on-line, Internet, 26 January 1997, available from http://pathfinder.com/@@LL1c6QYAspdOHaCM/time/magazine/domestic/1995/950821.cover.html.

12. Peter Grier, "Information Warfare," *Air Force Magazine* 78, no. 3 (March 1995): 34.

13. Richard J. Newman, "Warfare 2020," *U.S. News and World Report* 121, no. 5 (5 August 1996): 35.

14. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 15.

15. US Air Force Doctrine Document (AFDD) 1, "Air Force Basic Doctrine," 21 May 1996 (second draft), 9.

16. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 90. The concept of defeating an adversary's will and capacity to make war may be traced to the writings of Carl von Clausewitz as he defined three broad objectives of war "which between them cover everything: the *armed forces,* the *country,* and the *enemy's will*." This concept has permeated US military thinking as demonstrated by its inclusion in military doctrine, including Joint Pub 3-0, *Doctrine for Joint Operations,* 1 February 1995; US Army Field Manual (FM) 100-5, *Operations,* June 1993; Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force* , vol. 1, March 1992; and AFDD 1.

17. FM 100-6, *Information Operations,* August 1996, 1–12.

18. Col Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review,* November 1994, 42.

19. Stein, "Information Attack," 114.

20. John R. Boyd, "A Discourse on Winning and Losing," briefing slides, Air War College, Maxwell AFB, Ala., August 1987. Boyd's "observation-orientation-decide-act" (OODA) loop is based on the concept that "every individual operates an OODA loop that is unique in speed and accuracy. Speed is based on the individual's mental capacity and capability to deal with information and changing environments. John Boyd asserts that one can paralyze an enemy by operating inside the opponent's OODA loop, meaning that the individual is operating a faster cycle speed than the enemy's. Accuracy is determined during the orient part of the cycle by what information is filtered and how it is organized. Boyd considers the orientation as the most important part of the cycle because 'it shapes the way we interact with the environment—hence orientation shapes the way we observe, the way we decide, the way we act.' " This description of Boyd's OODA loop is taken from "Information Operations: A New War-fighting Capability," Lt Col William Osborne et al., in *2025 White Papers: Power and Influence,* vol. 3, bk. 1, 49.

21. Stein, "Information Attack," 114. Stein explained that "in many cases, indirect IW will be platform-to-platform as, for example, offensive and defensive electronic warfare, jamming or

other interference systems, and psychological operations via the successor systems to *Commando Solo*. It may, however, rely on nonelectronic old-fashioned military deception and psychological operations."

22. Ibid. Stein described corruption of the "orientation" portion of the OODA loop: "adversary analysis, whether artificial-intelligence or information-technology based or, most importantly, based in the mind of the human decision maker, decides and acts with full confidence in either the information observed or the integrity of his (machine or human) analytic processes."

23. Ibid.

24. Col Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 60.

25. Ibid., 44.

26. *Cornerstones of Information Warfare*, 4.

27. Ibid.

28. Ibid.

29. Sumner Benson, "How New the New Russia? Deep-Strike Weapons and Strategic Stability," *Orbis*, Fall 1996, 509.

30. Col John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 43.

31. Ibid.

32. Clausewitz, 184.

33. Eduard Mark, *Aerial Interdiction: Air Power and the Land Battle in Three American Wars* (Washington, D.C.: Center for Air Force History, 1994), 363. Mark explains that "the greatest single advantage of the Communists in resisting interdiction, other than their low logistical requirements, was that they were usually free to give battle or to decline it at will."

34. Earl H. Tilford Jr., "The Prolongation of the United States in Vietnam," in *Prolonged Wars: A Post-Nuclear Challenge*, ed. Dr. Karl P. Magyar and Dr. Constantine P. Danopoulos (Maxwell AFB, Ala.: Air University Press, 1994), 371 and 389. Tilford proclaims that "Hanoi won the Vietnam War." He explains that North Vietnam and the Vietcong forces sustained their will to fight. "For the communists, their fight with the United States and the Saigon regime was purposeful. Their objectives were constant, achievable, and better defined. Their political and military leaders, in working to achieve those objectives, devised superior strategies which, eventually, produced victory. The communists wanted to make the Americans suffer—over an extended period of time—until they gave up."

35. TSgt Pat McKenna, "Info Warriors: Battling for Data Dominance in the Fifth Dimension," *Airman Magazine*, September 1996, n.p.; on-line, Internet, 22 January 1997, available from http://www.af.mil/pa/airman/0996/info.htm.

36. Thomas A. Keaney and Eliot A. Cohen, *Revolution in Warfare? Air Power in the Persian Gulf* (Annapolis, Md.: Naval Institute Press, 1995), 236–37.

37. James P. Coyne, *Airpower in the Gulf* (Arlington, Va.: Aerospace Education Foundation, 1992), 190.

38. Michael R. Gordon and Gen Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston, Mass.: Little, Brown and Co., 1995), 246–48; and Steven K. Black, "Information Warfare in the Post–Cold War World" (paper submitted as part of the Air Force Fellow Program to the Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, 1996), 16.

39. John R. Levine and Carol Baroudi, *The Internet for Dummies*, 2d ed. (San Mateo, Calif.: IDG Books Worldwide, Inc., 1994), 12. The authors ask, "Can the Internet really resist enemy attack?" and answer, "It looks that way. During the Gulf War in 1991, the US military had considerable trouble knocking out the Iraqi command network. It turned out that the Iraqis were using commercially available network routers with standard Internet routing and recovery technology. In other words, dynamic rerouting really worked. It's nice to know that dynamic rerouting works, although perhaps this was not the most opportune way to find out."

40. Keaney and Cohen, 60.

41. Col Trevor N. Depuy, *A Genius for War* (Fairfax, Va.: Hero Books, 1984), 4. Also R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* 9, no. 4 (Winter 1995): 76.

42. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, Calif.: RAND, 1996), 22–23. Perception management is "manipulating information that is key to perceptions."

43. Stein, "Information Attack," 91, 114. Dr. Stein states, "Information attack is not so much perception management as orientation management. Information is both the target and the weapon; the weapon effect is predictable error."

44. Szafranski, 45.

45. Stein, "Information Attack," 91, 114.

46. Richard Overy, *Why the Allies Won* (New York: W. W. Norton & Co., 1995), 13.

47. Ibid., 151.

48. Szafranski, 42.

49. Thomas B. Allen and Norman Polmar, *Code-Name Downfall: The Secret Plan to Invade Japan and Why Truman Dropped the Bomb* (New York: Simon & Schuster, 1995), 258–89.

50. Gordon and Trainor, 246–48. Also, Black, 16.

51. Depuy, 4. Also DiNardo and Hughes, 76.

52. McKenna, n.p.

53. Several noted authors have warned of this phenomenon regarding the US fascination with technology and with finding a silver-bullet weapon that allows quick victory with minimum collateral damage. They include Earl H. Tilford Jr., *The Revolution in Military Affairs: Prospects and Cautions*, report (Carlisle Barracks, Pa.: Strategic Studies Institute, US Army War College, 23 June 1995), 4; Charles J. Dunlap, "How We Lost the High-Tech War of 2007: A Warning from the Future," *The Weekly Standard* 1, no. 19 (29 January 1996): passim; DiNardo and Hughes, 69; and Black, 1.

54. John A. Tirpak, "Shifting Patterns of Air Warfare," *Air Force Magazine* 80, no. 4 (April 1997): 26.

55. Capt George A. Crawford, "Information Warfare: New Roles for Information Systems in Military Operations," *Air Chronicles*: n.p.; on-line, Internet, 26 January 1997, available from http://www.cdsar.af.mil/cc/crawford.html.

56. Eliot A. Cohen, "Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March/April 1996): 51. Cohen is professor of strategic studies at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

57. Frank C. Mahncke, "Information Warriors," *Naval War College Review* 47, no. 3 (Summer 1994): 133. This piece appeared as a book review of the Tofflers' *War and Anti-War: Survival at the Dawn of the 21st Century*.

58. Richard W. Aldrich, "The International Legal Implications of Information Warfare," INSS Occasional Paper 9 (US Air Force Academy, Colo.: Institute for National Security Studies, April 1996), 1 and 16.

59. Ibid., vii.