The Law and the Human Target in Information Warfare: Cautions and Opportunities

Charles J. Dunlap, Jr.

Americans, including many wearing uniforms, often tend to misperceive the nature of war. They are inclined to oversimplify it into a rather mechanistic process that considers "body counts" and the destruction of a given number of objects as indicative of success. The true essence of war is, however, intellectual. As the military theorist Carl von Clausewitz observed, war is an act intended "to compel our enemy to do our will"[1] Thus, all warfare—to include Information Warfare[2]—is essentially a contest of wills between the living. Yielding to the will of another is fundamentally a cerebral process.

Information is the key to the mental interaction that underlies human conflict so conceived. It provides the raw material by which the human mind calculates its interests and decides whether or not to submit its will to its foe. As I will discuss, we in the West, and particularly the United States, do not always do a very good job of correctly perceiving what, in fact, a particular adversary considers to be his "interests", or even the kind of information used in that analysis.

Still, it is clear that the ability to shape the information upon which an adversary relies is an immense advantage in modern war. Correspondingly, controlling the information that influences the calculations made by one's own side is equally important. The type and accuracy of the data used, for example, to determine victory or defeat in a given circumstance is obviously a critical element for leaders to know and appreciate.

Moreover, information provided to the public can be decisive as to the support a military effort enjoys. If public support—particularly in liberal democracies—collapses, the military operation will likely end in short order. In Clausewitzean terms[3] this means that information-and especially that which influences the all-important public opinion-is one of the centers of gravity[4] in today's conflicts. Because of the importance of information to both sides in a belligerency, one might fairly argue that all war is, in the end, Information Warfare in some way.

Thus, in a very real sense the human target, that is, the collective mindset of the adversary, is the most lucrative target in virtually all wars (excepting perhaps wars of annihilation). Historically, U.S. and other Western militaries have sought to influence the mindset of adversaries by, quite literally, eliminating their capability to physically resist[5]. This usually required the actual destruction of the bulk of the enemy forces. For a variety of reasons, this will seldom be feasible in the future: few governments (certainly among the principal Western powers) could tolerate the enormous dedication of time and resources—that not to mention casualties and the attendant political capital—that this approach requires. Indeed, for potential foes of the United States, such a strategy is inconceivable in the near-term, given America's current military prowess and considerable resources.

Accordingly, for the foreseeable future, opponents of the United States will wage a kind of "ritual war" in which combat engagements are as much or more important for their symbolic value as they are for whatever actual effect they may have on a foe's order-of-battle. Both sides in such conflicts will find that the real struggle will occur, not on the battlefield *per se*, but in the minds of the combatants and those that support them. In other words, there will be few future wars where an enemy is forced to yield because his physical military capability has been fully exhausted; instead they will be strategic contests to win "hearts and minds".

Given the centrality of the information in such conflicts, it is imperative that decision-makers understand the importance of observing the Law of Armed Conflict (LOAC)[6] While one would hope this would be instinctive to both military and civilian leaders, it is becoming ever-more apparent that the new realities of late 20th century politics are, in any event, mandating adherence. The communications revolution is increasingly providing the masses with real-time access to information from war zones. Publics now—and to an even greater extent in the future—have the ability to easily monitor the conduct of their militaries, uncensored by government handlers through a technology-empowered media. This information flow and the perceptions it can create have real potential to significantly affect the ability of liberal democracies to wage war. Professors W. Michael Reisman and Chris T. Antoniou explain.

> In modern popular democracies, even a limited armed conflict requires a substantial base of public support. That support can erode or even reverse itself rapidly, no matter how worthy the political objective, if people believe that the war is being conducted in an unfair, inhumane, or iniquitous way.[7]

I would contend, therefore, that LOAC has as much rationale in the Machiavellian ethic of modern politics as it does as any classical construct of morals or virtue. Accordingly, I believe it is in the interest of Information Warfare advocates to be conscious of what the law does or does not permit if, for no other reason than the failure to be sensitive to these concerns may well lead to operational failure.

The purpose of this essay is essentially set forth in the title. To be more specific, it will: 1) briefly examine the current state of the law as it applies to the use of Information Warfare (IW) methodologies against the human target, and 2) try to forecast emerging issues and trends. In so doing, it will touch on Information Operations (IO) issues that arise during periods of putative peace, but will focus mainly on (IW)[8] matters, that is, "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[9]

The Legal Regime

Perceived wisdom in some quarters holds that the whole subject of IW is so new that no existing legal regime applies. *This is simply incorrect.* While it may be that there are certain areas where the law needs development or clarification, a surprising amount of existing law quite clearly does apply to IO. This is especially true with respect to the human target.

Still, the legal architecture applicable to IO involving the human target is admittedly complex. Some of the complicating elements include the fact that legality of a particular

action may depend upon where on the temporal spectrum-of-conflict it is used, as well as against exactly whom it is targeted. For example, a covert peacetime Information Operation directed against non-state actors (e.g., terrorists or drug dealers) is subject to a rather different body of law than psychological operations (psyops)[10] aimed against lawful combatants in an international armed conflict.

The aforementioned phrase "international armed conflict" is itself of great import. As a general rule, LOAC-like most international law-applies to relations between nations, not individuals or other non-state actors. It does not ordinarily apply to situations such as law enforcement operations (though the U.S. Department of Defense (DoD) as a matter of policy will usually apply it to all operations involving its personnel[11]). Parenthetically, enthusiastic designations of a government effort as being a "war on drugs" or a "war on terrorism", (some non-governmental entities even anoint themselves with appellations like "soldiers" or "armies"), are not dispositive as to legal status under LOAC. The fact is that LOAC does not usually control or limit operations against what, from a legal perspective, are simply individuals or groups engaged in criminal enterprises.

Nevertheless, the indiscreet use of martial metaphors, combined with the employment of military resources targeted at non-state actors, is a matter of some concern. When IO advocates insist, for example, that they are engaged in an ongoing "cyberwar", it is not inconceivable that some day the international community will take that rhetoric at face value. This is not something with which we should necessarily take comfort. It is not, in my view, in the interest of the United States or other developed nations to have the machinations of non-state actors dignified as acts of combatants covered by LOAC. Among other things, this may mean that the perpetrators of various crimes might be able to claim the immunity afforded combatants under international law for acts committed *in bello*[12]

In any event, it would be a mistake to assume that IO conducted outside of an international armed conflict is free of legal limitation. To the contrary, in many instances the legal limits are even greater because a myriad of international agreements—many international telecommunications agreements aimed at facilitating the free flow of information[13]—are applicable to the facilities information operators seek to employ.[14] As a general proposition, these international regulatory schemes are aimed at ensuring, among other things, that international communication and other data transfers remain free from harmful interference. The United States, along with other parties to these agreements, have implemented domestic legislation requiring compliance with them, and these laws often impose criminal penalties.[15]

Indeed, the most serious limitation on IO activities against human targets in peacetime is, in the U.S. anyway, domestic law. A range of Federal and state statutes exist that, for example, criminalize various computer-intrusion acts,[16] the very practices that information operators may wish to employ. Except to the extent that some (but not all) contain exceptions for surveillance activities by law enforcement and intelligence agencies, these laws apply to military personnel and other government personnel to the same extent as anyone else. There is no blanket "national security" exception to the criminal laws, as many seem to believe. Furthermore, authority to monitor information systems does not necessarily include the power to manipulate or seize data within them, absent compliance with applicable judicial prerequisites. In this regard it is important to

recall that military personnel are generally prohibited from engaging in domestic law enforcement activities via IO or otherwise.[17]

In the United States, laws controlling covert actions [18] that is, any activity aimed "to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. will not be apparent or acknowledged publicly"[19] are quite strict. Many kinds of IO aimed at the human target could fall within their purview. Of particular interest is the absolute prohibition on covert actions "intended to influence United States political processes, public opinion, policies, or media."[20]

Covert action laws do not, however, limit "traditional military activities" or IO where the role of the U.S. is apparent or acknowledged. Public information and public diplomacy programs are legal and may target audiences both here and abroad. It appears, however, that many of these efforts are less than deft. In the aftermath of Kosovo, where such operations appear to have had limited success, it is reported that the United States has established a new organization intended to improve performance in this area.[21]

In this respect it may behoove military organizations to resist the trumphalism that has marked too many public briefings in recent years. Consider, for example, the many showings of precision-guided munitions slamming precisely into what are very obviously purely military targets. The net effect—and presumably unintended consequence—of this carefully selected footage has been to feed public anticipations of the unattainable "immaculate war." Once public expectations are raised, difficulties are created when the "friction of war" causes unintentionally misdirected weapons.

Despite NATO's insistence that it achieved over 96% accuracy during operations against Yugoslavia, it is instructive to note that repeated scenes of civilian casualties paralleled a progressive drop in public support for the air campaign.[22] Even more problematic is the fact that the overselling of technological capabilities creates a perception of deliberateness when mistakes inevitably do occur. Consider that following the attack on the Chinese Embassy the tenor of evening news reports on the national television networks shifted drastically from 58% of the stories having a favorable character to 86% of them being negative in tone.[23] Under these circumstances it should not have been as much of a surprise as it was to many that at the end of the campaign a majority of Americans did not consider the outcome a U.S. victory.[24]

Efforts to educate the public as to the realities of war are becoming ever more important, since a smaller percentage of the population has served in the armed forces or even knows anyone who has served in the military.[25] Once the conflict begins, it may be too late to succeed in this process, and even the attempt to do so may appear too self-serving. Of course, this presumes that there is a bright-line definition of when war begins in the Information Age.

Information Operations during Armed Conflict

Cyber-warriors frequently ask some permutation on the following query: "what is an act of war in the Information Age?" Actually, the phrase "act of war" is outmoded. From a legal perspective, there are only two bases to use armed force subsequent to the ratification of the UN Charter that, in essence, outlawed war. The two situations still authorizing the use of armed force are: 1) pursuant to a UN Security Council Resolution;

or 2) in self-defense in response to an "armed attack" pursuant to Article 51 of the Charter. However, in the post-Kosovo era we may yet see the development of a third basis, that being the humanitarian intervention rationale.[26]

Clearly, these concepts, and especially Article 51, are largely predicated on the assumption that "armed attacks" and similar provocations will employ kinetic weapons. The legal situation is less clear when the "attack" occurs digitally and consists merely of the manipulation of data. Nevertheless, there appears to be a growing consensus among international lawyers, at least insofar as computer network attacks are concerned. An "armed attack" for the purposes of Article 51 is considered to have occurred when the characteristics and effects of the cyber-strike equate to those that result from a traditional kinetic weapon attack.[27] Importantly, *digital espionage via computer or similar means does not, per se, violate international law, though it may breach domestic law of the targeted nation.* As Professor Gary Sharp has pointed out, however, *such action might under certain circumstances be interpreted as an expression of hostile intent so as to provoke an anticipatory self-defense response.*[28]

In any event, regardless of the particular manner in which an international conflict is initiated, once it has begun, LOAC applies. As a general principle of international law most agreements are suspended between belligerents, unless they are explicitly written to remain in effect during wartime.[29] Thus, it can be argued that many of the international communications agreements previously discussed do not limit the information operator's options in times of war. However, certain agreements to include, for example, the Hague and Geneva Conventions,[30] do, in fact, apply to the IO conducted against the human target during periods of international armed conflict. Besides treaties, a fairly well-developed body of customary international law[31] applies to IO against the human target, as it does to other means and methods of warfare.

While it is beyond the scope of this essay to enumerate all the many aspects of LOAC, it is worth noting that, with respect to the human target, one of its most basic principles is that the "*rights of belligerents to adopt means of injuring the enemy is not unlimited.*"[32] There are other basic concepts that apply to the human target in IW, just as they do to other targets in more conventional conflicts. These would include the principles of *discrimination* and *proportionality.*

Discrimination requires the means or method of warfare to distinguish between combatants and noncombatant persons and objects. This presents a real challenge to cyber-warriors who wish to employ certain methods of computer attack, because LOAC requires that these methods be capable of discrimination.[33] The principle of *proportionality* requires that the collateral damage to noncombatants or their property not be disproportionate in relation to the "concrete and direct military advantage anticipated."[34] It is also important to understand that LOAC does not favor either side; that is, the presumed "righteousness" of a side, even if patently obvious, nevertheless does not allow it any greater freedom of action. Further, LOAC explicitly rejects an "ends justifies the means" approach to warfare-called Kriegsraison in the law.[35]

In other words, *even if a particular information operation targeting a human being might bring a given conflict to an early termination, its execution is still forbidden if it is violative of LOAC.* The reason for this is obvious: were they not the case, war would

quickly descend to a level of savagery that would not facilitate the restoration of peace, which is one of the fundamental purposes of LOAC. The enmity that *Kriegsraison* generates is not unlike that which fuels the seemingly endless cycle of ethnic violence that we see around the world today.

LOAC anticipates developments in the means and methods of warfare. Further, Protocol I to the Geneva Conventions of 1949, like several earlier treaties, contains what is called a "Martens Clause". This clause holds that in "cases not covered by this protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of the public conscience."[36]

The prohibition against attacks directed against civilian objects is an important concept for information warriors to consider in constructing strategies against the human target. Too often we see suggestions in the literature—or even press reports—about computer network attacks aimed, for example, against the personal bank accounts of adversary leaders.[37] Absent a showing that such monies are being directly used to support a military effort, it would seem that such a tactic could not be reconciled with LOAC. Additionally, some experts believe that such attacks would invite retaliation to which the U.S. is vulnerable, and thus expose the attackers to legal liability if third-party banks are struck.[38]

A more complex problem is presented by the use of IO techniques such as a computer network attack against dual-use infrastructure targets. Because many of these facilities use computer-driven controls, they are often touted by information warriors as especially lucrative opportunities to substitute digital attack for a conventional military strike.[39] However, in many cases both military forces and civilian society rely upon the same power grid, communications network, transportation links, and fuel supply system. Modern societies, especially in the urbanized setting, are extremely vulnerable to such infrastructure loss. For example, destroying the power grid may well deny military facilities with necessary power, but at the same time leave the noncombatant civilian population without water, sewerage, heat, transportation and other systems essential for life.

In order to attack such targets consistent with LOAC, a proportionality analysis must be accomplished. It is, of course, not impermissible to conduct infrastructure attacks if there is a sufficiently overarching military objective, and the expected collateral damage is incidental. However, simply because few, if any, *immediate* casualties may result,[40] that does not mean the significant secondary or reverberating affects upon the noncombatant population can be overlooked.[41] Still, as indicated above, such attacks are permissible where the military advantage sought outweighs the expected collateral effects upon noncombatants (inclusive of the reasonably foreseeable reverberating effects).

A troubling precedent with respect to infrastructure attacks appears to be emerging in the aftermath of Kosovo. According to a 25 May 1999 report in *The Washington Post*, NATO officially insisted that attacks on the power grid were intended to disrupt the Yugoslav military, but "senior allied military officials acknowledged that they also wanted to damage the quality of everyday life so that suffering citizens will start questioning the intransigence of their political leadership."[42] It appears that this strategy worked. Thomas L. Friedman wrote in the *New York Times* that:

> As the Pentagon will tell you, airpower alone brought this war to a close in 78 days for one reason-not because NATO made life impossible for Serb troops in Kosovo (look how much armor they drove out of there), but because NATO made life miserable for the Serb civilians in Belgrade.[43]

Following the conflict, *Airman Magazine*, an official publication of the U.S. Air Force, published the following comments from the senior Air Force commander during the campaign:

> "As an airman, I would have targeted the power grid, bridges and military headquarters in and around Belgrade the first day of the conflict," said [the commander], who believes that's what eventually brought Milosevic to his knees. "Air power is made for shock value."
>
> "Just think if after the first day, the Serbian people had awakened and their refrigerators weren't running, there was no water in their kitchens or bathrooms, no lights, no transportation system to get to work, and five or six military headquarters in Belgrade had disappeared, they would have asked: All this after the first night? What is the rest of this [conflict] going to be like?"[44]

Destroying infrastructure—whether by conventional bombing or via digital attack—in order to deny noncombatants an indispensable necessity of life like water, to leave them with spoiled food in a wartime economy, and to deny them transportation without regard to the nature of their work, is not the kind of attack that is, in my opinion, permissible under LOAC.[45] Although the actual attacks conducted during the Yugoslav operation appear justified as bona fide efforts to reduce the effectiveness of military facilities and military equipment and communications, a number of groups condemned the NATO bombing campaign.[46] If the purpose was that hypothesized in the *Airman Magazine*, then the critics' complaints could have substance.

In short, *when the human target is a noncombatant, then attacks for the sole purpose of eroding their life support system are impermissible, regardless of the methodology employed. This is not to say, however, that noncombatants cannot be inconvenienced or denied the luxuries.* However, as Yves Sandoz of the International Committee of the Red Cross observes, defining the "military advantage when the aim of the operation is to weaken the enemy so as to make him surrender" is extremely problematic.[47]

Apart from the legal and moral issues generated by infrastructure attacks, consider a 1994 study by the U.S. Air Force's School for Advanced Aerospace Studies entitled "Strategic Attack of National Electrical Systems".[48] After reviewing WW II, Korea, Vietnam, and especially the Gulf War, the study concludes that: "To strike electric power to affect civilian morale, increase costs to leadership, or impact the military will waste missions and could prove counterproductive to the political aims of the war..."[49]

The study goes on to say with respect to Iraq, where damage to the electrical grid was blamed for thousands of noncombatant deaths, that "the practical fact is the negative impact of these attacks on world opinion far outweighed the military benefits accrued by bombing electrical power in Iraq. The implication is clear—national electrical systems are not a viable target."[50] Thus, cyber-warriors should consider that attacks against dual-use infrastructure might undermine the public support that Clausewitz tells us is part of the "remarkable trinity" of war.

Computer network attack is not the only or even necessarily the most effective means of IW against the human target. Psychological Operations present real opportunities for the information operator, as there are relatively few legal limitations. One example of an unlawful psyop would be "to broadcast a false report of cease-fire or armistice", which in LOAC terms is impermissible perfidy.[51] That said, it is not—despite what many people think—violative of LOAC to use lies or disinformation that do not amount to perfidy. Nevertheless, as a matter of DoD policy, "[d]eception operations will not intentionally target or mislead the US public, the US Congress, or the US media."[52] Sidney Axinn, however, argues in his book *A Moral Military*:

> [What is] the morality of psychological warfare? When it is an effort to use the truth to gain a military goal, this type of warfare is to be accepted and applauded. When lying or "disinformation" is used, it cannot be accepted as an honorable weapon. (Of course, this is quite apart from legitimate tactics to conceal information from an enemy or to mystify or fool an enemy.)[53]

In any event, some experts insist that there "is no need to lie because properly packaged, the truth is the very best propaganda."[54] Nonetheless, because technology now permits the digital manipulation of photographs and film to create extraordinarily convincing but false images,[55] information warriors see unique opportunities to assail the human target, especially enemy leaders.[56] Thomas Czerwinski, then a professor in the School of Information Warfare and Strategy at the National Defense University, asks: "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?"[57] Quite obviously, they could deceive a population about its leaders, as Professor Czerwinski indicates.

While propaganda of this sophistication may be new, the idea of using psyops to undermine an adversary's leaders is not. But this norm may need re-examination when the government affected is a democratic one. A key component of U.S. national security policy is the promotion of democracy.[58] While no one would dispute that the improper actions of the leaders of any adversary state-including those of democracies-must be stemmed, it is something altogether different to hold that it is an appropriate strategy to attempt to change democratically-elected leadership via the dissemination of manipulated information.

Furthermore, Michael Walzer asserts that "war aims legitimately reach to the destruction or defeat, demobilization, and (partial) disarming of the aggressor's armed forces. Except in extreme cases, like that of Nazi Germany, *they don't legitimately reach to the transformation of the internal politics of the aggressor state or the replacement of its regime*."[59] Surely, a democratic government is not the kind of extreme case that Walzer exempts. Thus, for policy reasons beyond any short-term gain, it may be prudent to restrain information warriors from engaging in tactics that damage the democratic process.

With respect to non-democratic governments, psyops aimed at undermining them are not necessarily unlawful, even if it is reasonably expected that civilian casualties may result. For example, it has long been permissible under LOAC to attempt to induce a civil insurrection in an adversary nation [60] despite experience that shows that civil wars can have horrific effects on civilian populations. The key here is that the appalling nature

of modern civil wars is much the result of excesses committed by security forces. LOAC does not, itself, impose legal obligations upon the propagator of the psyop for crimes the security forces may commit.

The real limitation on the effectiveness of psyops is not so much the law, but the fact that Americans too often do not properly evaluate the human target. Edward L. Rowney, a former U.S. arms control negotiator and retired Army general comments:

> Our biggest mistakes stem from the assumption that others are like us, when in fact, they are more unlike than like us. We insist on ascribing to others our cultural traits, not recognizing that we have different objectives due to our unique historic backgrounds and sets of values. In short, "We fail to place ourselves in the other person's moccasins."[61]

It is ironic that the nation that invented modern "Madison Avenue" methods of persuasion appears to struggle to develop effective cross-cultural psyops. According to one report, for example, psyops in the U.S.-led Yugoslav campaign were "boring and badly done-it [was] miserable."[62] One way of improving psyops attacks against the human target may be to relax legal requirements that talented information specialists must meet in order to become part of the armed forces. It may be wise to allow persons-the disabled and others-who have the psyops skills but who presently cannot do so join the armed forces or create a special reserve unit to accommodate them.[63]

An important part of psyops is denying the adversary the opportunity to conduct the kind of information campaigns that sustain the support of the people. As a general rule, journalists—even those attached to military units—are treated under LOAC as civilians,[64] so long as they do not do act inconsistent with that status, such as taking part in hostilities.[65] In the Kosovo conflict, Serbian broadcast radio and television outlets were bombed in an action criticized by a number of international lawyers[66] and organizations.[67] However, in this case the facilities were used to whip up ethnic hatreds for years.[68] As NATO spokesman, Air Commodore David Wilby, declared on April 8, 1999: "Serb radio and TV is an instrument of propaganda and repression...It is...a legitimate target in this campaign."[69] Indeed, incitement to genocide may itself be a war crime.[70] Under these circumstances I believe that propaganda outlets are legitimate targets for attack, provided the appropriate proportionality analysis sustains it.[71]

A rather more complex problem is raised by the dramatic growth in the capabilities of the media to report from war zones. Globalized news sources now have the technical means to rapidly gather and disseminate information about military operations virtually without support or censorship of governmental authorities. Moreover, commercial satellites-many of which are owned by third parties-are providing high-resolution images heretofore the exclusive province of the intelligence agencies of the developed nations.[72] Another information source, the Internet, is now being described as a "simple, low-cost, non-threatening and relatively risk-free" way of collecting data.

In short, the media and commercial information sources are becoming the "poor man's intelligence service", with the capability to provide information of great value to adversaries. Perhaps of even greater significance is the fact that much of this near-instantaneous information can complicate the political equation for democratic leaders.

The sheer speed with which it is conveyed gets inside the "decision loop" by presenting publics with raw data before leaders can prepare them to understand it in the context of an ongoing military operation.

As suggested above, it appears that if the military value of the information being transmitted to the enemy is sufficiently important, and the IW means employed to disrupt or corrupt that flow otherwise complies with LOAC principles—to include the concept of proportionality—it would seem permissible to conduct the operation. It may, however, be politically infeasible to do so if the operation raises the specter of confrontation with a media outlet from a non-belligerent third party not currently involved in the conflict.[73]

But what if the purpose of the operation is to disrupt the flow to a friendly "human target," our own public?[74] For example, in a report on the attacks on Serb television stations, Patrick L. Sloyan pointed out that while bombing stopped the "diet of lies fed Serb viewers," it also would "curb transmission to the West of those disturbing 'collateral damage' pictures that could erode public support for NATO's escalating strikes in the Balkans."[75] If the latter were the sole aim, would the attacks be justified? Probably not.

Censorship and exclusion of the press from military operations has long been tolerated in liberal democracies during wartime.[76] Essentially, where there is a demonstration that the information would present a clear and present danger to national security, it could be suppressed.[77] That concept, however, would not seem to permit the suppression of news reports via IW or other means, simply because the information conveyed would tend to demoralize public opinion.

Concluding Observations

This paper has sought to present an outline of the law as it relates to the human target in information warfare. Basically, IW should be considered and evaluated in much the same way as any other methods or means of warfare. In most instances, the application of LOAC is relatively straightforward and should not present the operator with significant difficulty.

Perhaps the most challenging of the emerging issues relates not so much to the fact that the technology may be new or has not heretofore been put to military uses, but to the fact that such developments have marked the history of warfare for eons. Rather, it relates to the increasing tendency of military commanders to attempt to directly shape public opinion in both adversary countries, as well as domestically. This represents a departure from the practice in the U.S. and many Western countries to leave such concerns largely to the civilian leadership. Still, to the extent this effort is based on a timely and well-conceived presentation of accurate facts, it cannot be criticized and may well serve to enhance the effectiveness of military operations.

However, where IW techniques are sought to manipulate or deny information, we must be concerned about the legitimacy of the effort. Modern communications technology makes it virtually impossible to segregate messages sent to adversary societies from that consumed by friendly publics. In addition, if IW techniques—and especially computer—network attack methodologies-are used to achieve ends against the human target that are impermissible if accomplished via kinetic weapons, they must be rejected.

Where the human target in IW is a noncombatant civilian, his person and property is entitled to protection under LOAC, and it is our duty to secure such persons and objects from attack. It is imperative that the lure of IW not result in a reemergence of *Kriegsraison*—like "we-had-to-burn-the-village-to-save-it" syndrome. Should that occur, we forfeit the very ideals for which we stake-as those who went before us did-"our Lives, our Fortunes, and sacred Honor."[78]

Endnotes

[1] Carl von Clausewitz, *On War* (Michael Howard and Peter Paret, (ed., and trans. 1976) (1832), p. 75.

[2] There are many possible definitions of Information Warfare, but a common official definition is that used by the Air Force, that is, "any action to deny, exploit, corrupt or destroy the enemy's information and its functions while protecting Air Force assets against those actions and exploiting its own military operations." See Captain Robert G. Hanseman, USAF, *The Realities and Legalities of Information Warfare*, 42 *A.F. L. Rev.* 173, 176 (1997) citing USAF Fact Sheet 95-20 (Nov. 1995). See also note 8 *supra* and accompanying text.

[3] Clausewitz held that war is a "remarkable trinity" composed of the people, the military, and the government. See Clausewitz, *supra* note 1, p. 89.

[4] Centers of gravity are "[t]hose characteristics, capabilities, or localities from which military forces derive freedom of action, physical strength, or will to fight." See Chairman of the Joint Chiefs of Staff, Joint Publication (Joint Pub) 1-02, *DoD Dictionary of Military and Associated Terms*, 23 March 1994, as amended 29 June 1999.

[5] See generally, Russell Frank Weigley, *The American Way of War : A History of United States Military Strategy and Policy* (1978) (discussing the strategy of annihilation that has marked U.S. wars).

[6] LOAC might be described as follows:

> LOAC is a body of law that derives from several international treaties (specifically, the Hague and Geneva Conventions), as well as customary international law (law created by the custom and practice of civilized warring states, which is binding on all nations). It applies to all armed conflicts between states (thus, civil wars or battles with terrorist groups are not covered.) Hague Law is concerned mainly with the means and methods of warfare, while Geneva Law is concerned with protecting persons involved in conflicts, such as POWs, the wounded, and civilians.
> Hanseman, *supra* note 2, p. 189.

[7] W. Michael Reisman and Chris T. Antoniou, *The Laws of War* xxiv (1994) (emphasis added).

[8] The Joint Chiefs of Staff define Information Warfare as "[a]ctions taken to affect adversary information and information systems while defending one's own." Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (9 October 1998), p. GL-7.

[9] Joint Pub 3-13, *supra* note 8, p.GL-7. See also note 2 *supra.*

[10] Psychological operations are defined as "[p]lanned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes or behaviors favorable to the originator's objectives." See Joint Pub 3-13, *supra* note 8, p. GL-10. Ideally, a psychological operation "reduces the morale in combat efficiency of the enemy troops and creates dissidence and dissatisfaction within their ranks. Psychological operations can promote resistance within a civilian populace against a hostile regime or to enhance the image of a legitimate government. The ultimate

objective of American psyops is to convince enemy, friendly, and neutral nations and forces to take action favorable to the U.S. and it's allies." Colonel Frank L. Goldstein, USAF, and Colonel Daniel W. USAF, Retired, "Psychological Operations: An Introduction" in *Psychological Operations: Principles and Case Studies* (Air University Press, Colonel Frank L. Goldstein, ed., 1996), p. 5.

[11] Department of Defense Directive 5100.7, DOD *Law of War Program*, July 10, 1979.

[12] Noel C. Koch, a former senior DOD official, argues that it would be "grotesque to afford terrorist the rights that belong to legitimate combatants under the laws of war." See: LtCol Richard J. Erickson, USAF, *Legitimate Use of Military Force Against State-Sponsored International Terrorism* (Air University Press, July 1989), p. 64 (Erickson, himself, however, argues that as unlawful combatants, terrorists are not afforded the rights of legitimate combatants. That view, however, is contingent upon particular facts and circumstances.)

[13] See *e.g.*, The International Telecommunications Satellite Organization Agreement (INTELSAT), 20 August 1971. For a discussion of the legal aspects of Information Warfare in the context of dual-use satellite communications systems see: Robert A. Ramey, *Space Warfare and the Future Law of War*, July 1999 (unpublished thesis submitted to McGill University, Canada), pp. 165-171.

[14] For example, the UN Convention on the Law of the Sea may prohibit unauthorized psyop broadcasts from sea-based platforms. See Joint Pub 3-13, *supra* note 8, p. I-13.

[15] For example, 47 U.S.C. ß 502 criminalizes the knowing and willful violations of "any rule, regulation, restriction, or condition made or imposed by any international radio or wire communications treaty or convention."

[16] See e.g., The Computer Fraud and Abuse Act of 1986 and the Computer Abuse Amendments of 1994, 18 U.S.C. ß1030 *et seq.* For a bibliography of Federal statutory and regulatory guidance, see: U.S. Department of Defense, Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (2d Ed. 4 July 1996). For a recent discussion of the applicability of the criminal law to Information Warfare, see: Major David J. DiCenso, USAF (Ret.), "IW Cyberlaw: The Legal Issues of Information Warfare", *Airpower Journal*, Summer 1999.

[17] The Posse Comitatus Act (18 U.S.C. ß1385) forbids the use of the military to "execute the laws."

[18] See generally 50 U.S.C. ß413, *et seq.*

[19] 50 U.S.C. ß413b(e).

[20] 50 U.S.C. ß413b(f).

[21] Ben Barber, "Group Will Battle Propaganda Abroad", *Washington Times*, July 28, 1999. (Discussing the newly established International Public Information Group designed "to enhance U.S. security, bolster America's economic prosperity and to promote democracy abroad").

[22] By 25 May 25 1999, CNN was reporting that 82% of Americans favored a suspension of the airstrikes. See Keating Holland, "Americans Want Temporary Halt to Airstrikes", May 25. In the same poll, the percentage of Americans favoring U.S. participation in the airstrikes fell from 61% on 15 April to 49%. For details of the earlier poll see Keating Holland, *Support for NATO strikes, and ground troops growing*, April 15, 1999.

[23] "Inside TV", *USA Today*, June 10, 1999, at 3D (citing a study by the Center for Media and Public Affairs).

[24] A poll of Americans revealed an "absence of any of the euphoria that followed the end of the Gulf War" and that "not even half-48 percent-believed the United States and its allies won the war". See: Richard Morin, "Americans Back Ground Troops", *The Washington Post*, June 16, 1999, p. 32.

[25] For a discussion of the implications of the reported "gap" between military and civilian societies occasioned by the declining percentage of the population with military services, see: Thomas E.

Ricks, "The Widening Gap Between the Military and Society", *Atlantic Monthly* (July 1997), p. 66. A major study is underway by the Triangle Institute for Security Studies to examine this thesis.

[26] Some international lawyers contend, however, that humanitarian intervention is not justified and that the action in Kosovo constituted aggression in the absence of explicit UN sanction. See: Walter J. Rockler, "War Crimes Law Applies to the U.S. Too", *Chicago Tribune*, May 23, 1999. See also: D.G. Kousoulas, "The Day After", *The Washington Post*, June 8, 1999, p. 19.

[27] See e.g., Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 *Columbia Journal of Transnational Law* 885 (1999) and Walter Gary Sharp, Jr., *CyberSpace and the Use of Force* (1999).

[28] Sharp, *supra* note 27, p. 132.

[29] See Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 4. [Hereinafter "Assessment"].

[30] These include, the Hague Convention No. III Relative to the Opening of Hostilities, 18 October 1907; the Hague Convention No. IV Respecting the Laws and Customs of War on Land and Annex Thereto Embodying Regulations Respecting the Law and Customs of War on Land, 18 October 1907; the Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907; the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949; the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949; the Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949; and the Geneva Convention Relative to the Protection of Civilians in Time of War, 12 August 1949. See Department of the Army Pamphlet 27-1, *Treaties Governing Land Warfare* (7 December 1956).

[31] The International Military Tribunal at Nuremberg described "customary" international law in the context of LOAC as follows:

> The law of war is to be found not only in treaties, but also in the customs and practices of states, which gradually obtained universal recognition, and from the general principles of justice applied by jurists and practiced by military courts. This law is not static, but by continual adaptation follows the needs of a changing world.

As cited in Reisman and Antoniou, supra note p. xix.

[32] Article 22, Regulations Respecting the Laws and Customs of War on Land, annexed to Hague Convention IV, October 18, 1907.

[33] See generally: Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law* (1998), pp. 30-35, and Mark Russell Shulman, *Legal Constraints on Information Warfare*, Occasional Paper No. 7, Center for Strategic and Technology, Air War College, Air University, Maxwell Air Force Base, AL (March 1999), pp. 11-18.

[34] The concept of proportionality was codified in the 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, arts. 51.5(b) and 57.2(iii). [Hereinafter "Additional Protocol I"]. While the U.S. has not ratified Additional Protocol I, this portion is considered part of customary international law.

[35] *Kriegsraison* is the 19th century German doctrine that asserted that military necessity could justify any measure—even violations of the law of war. See Department of the Air Force, Pamphlet 110-31, *International Law-The Conduct of Armed Conflict and Air Operations* (19 November 1976), paragraph 1-3a(1).

[36] Article 1 (2), Additional Protocol I, *supra* note 34.

[37] See e.g., Gregory L. Vistica, "Cyberwar and Sabotage", *Newsweek*, May 31, 1999, p. 38 (alleging a

CIA cyberwar against Serbian President Slobodan Milosevic's bank accounts). See also: Douglas Waller, "Onward Cyber Soldiers", *Time*, August 21, 1995, p. 38 (reporting about an Army officer who discussed "electronically zero[ing] out" and enemy leader's bank account in a future war).

[38] See Bob Sullivan, "Cyberwar? The U.S. Stands to Lose", MSNBC, June 3, 1999.

[39] See Waller, *supra* note 37 (reporting about an Army officer who contended that he could win a war "almost bloodlessly" at a computer terminal. He visualized the foe's phone system brought down by a computer virus, logic bombs ravaging the transportation network, false orders confusing the adversary's military, the opponent's television broadcasts jammed with propaganda messages, and the enemy leader's bank account electronically zeroed out).

[40] See Winn Schwartau, "The Ethics of Civil Defense and Information Warfare", *Journal of the National Computer Security Association* (NCSA News), June 1997, pp. 15-17.

[41] See: Commander James W. Crawford, "The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems", 21 *Fletcher Forum of World Affairs* 101 (Summer/Fall 1997) (discussing secondary and reverberating effects).

[42] Phillip Bennett and Steve Coll, "NATO Warplanes Jolt Yugoslav Power Grid", *Washington Post*, May 25, 1999, p. 1.

[43] Thomas L. Friedman, "Was Kosovo World War III?", *New York Times*, July 2, 1999.

[44] As quoted by MSgt Tim Barela in "To Win a War", *Airman Magazine*, September 1999, pp. 2-3. These are essentially the same points reported earlier by the *The Washington Post*. See William Drozdiak, "Air War Commander Says Kosovo Victory Near", *Washington Post*, May 24, 1999, p. 1.

[45] Article 54, Additional Protocol I, *supra* note 34, makes it prohibited "to attack, destroy, remove or render useless objects indispensable for the survival of the civilian population" for "any motive."

[46] Fred Hiatt, "NATO's Good Fight", *The Washington Post*, July 11, 1999, p. B7.

[47] Yves Sandoz, "Beware, The Geneva Conventions Are Under Fire", *International Herald Tribune*, July 14, 1999.

[48] Major Thomas E. Griffith, Jr., USAF, *Strategic Attack of National Electrical Systems*, U.S. Air Force's School for Advanced Aerospace Studies, Air University, Maxwell Air Force Base, AL (October 1994).

[49] *Supra* note 48, p. 53.

[50] *Ibid.*

[51] Assessment, *supra* note 29, p. 7.

[52] Chairman, Joint Chiefs of Staff, Joint Pub 3-58, *Joint Doctrine for Military Deception* (31 May 1996), p. I-4.

[53] See Sidney Axinn, *A Moral Military* (1989). pp.159-160

[54] Colonel Fred W. Walker, USAF (Ret.), "Strategic Concepts for Psychological Operations", in *Psychological Operations: Principles and Case Studies*, *supra* note 10, pp. 17, 24.

[55] See Dennis Brack, "Do Photos Lie?", *Proceedings*, August 1996, p. 47.

[56] The author has previously discussed this theme. See Charles J. Dunlap, Jr., "Technology: Recomplicating Moral Life for the Nation's Defenders", *Parameters*, Autumn 1999, pp. 24, 37-38.

[57] As quoted by Peter Grier, "Information Warfare", *Air Force Magazine*, March 1995, p. 35.

[58] The White House, *A National Security Strategy for a New Century* 19 (May 1997).

[59] Michael Walzer, *Just and Unjust Wars* xvii (2d ed., 1992) (emphasis added).

[60] See Department of the Army, Field Manual 27-10, *The Law of Land Warfare* (July 1956), para 49, p. 22. See also, Greenberg, Goodman, and Soo Hoo, *supra* note 33, p. 35.

[61] Edward L. Rowney, "Tough Times, Tougher Talk", *American Legion Magazine*, May 1997, pp. 24-26.

[62] Carlotta Gall, "NATO TV Is Sent To Serbs, Who Are Harsh Critics", *New York Times*, May 26,

1999. Cf. Steven Collins, "Army PSYOP in Bosnia: Capabilities and Constraints", *Parameters*, Summer 1999, p. 57 (discussing the mixed record of PSYOP in Bosnia).

[63] The author discussed the benefits and perils of such a proposal in a paper entitled "Organizational Change and the New Technologies of War", presented at the Joint Services Conference on Professional Ethics, Washington, DC (January 1998).

[64] Articles 79, Additional Protocol 1, *supra* note 34.

[65] See Leslie C. Green, *The Contemporary Law of Armed Conflict* (1993), p. 233.

[66] Rockler, *supra* note 26.

[67] See William M. Arkin, "Changing the Channel in Belgrade", *The Washington Post*, May 25, 1990, (citing the Committee to Protect Journalists and Human Rights Watch).

[68] See *e.g.*, Jamie F. Metzl, "Information Intervention", *Foreign Affairs*, November/December 1997, p. 15.

[69] See Arkin, *supra* note 67.

[70] See Greenberg, Goodman, and Soo Hoo, *supra* note 33, p. 36, n.96 and accompanying text.

[71] According to the DoD General Counsel, "[w]hen it is determined that civilian media broadcasts are directly interfering with the accomplishment of the military force's mission, there is no law of war objection to using minimum force to shut it down." See Assessment, *supra* note 29, p. 9.

[72] See William J. Broad, "Private Ventures Hope for Profits on Spy Satellites", *New York Times*, February 10, 1997, p. 1.

[73] Compare Frederick W. Kagan, "Star Wars in Real Life: Political Limitations on Space Warfare", *Parameters*, Autumn 1998, p. 112.

[74] With respect to *adversary* news outlets, the DoD General Counsel states that the "extent to which force can be used for purely psychological operations purposes, such as shutting down a civilian radio station for the sole purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community." See Assessment, *supra* note 29, p. 9.

[75] Patrick L. Sloyan, "The Fog of War", *American Journalism Review*, June 1999.

[76] See generally, John Calvin Jeffries, Jr., "Excluding the Press form Military Operations", in *National Security Law* (John Norton Moore, Frederick S. Tipson, and Robert F. Turner, eds., 1990), p. 993.

[77] See generally, Donald L. Robinson, "National Security" in *The Oxford Companion to the Supreme Court* (1992) p. 574.

[78] The Declaration of Independence (U.S. 1776).

The views expressed in this article are those of the author and do not reflect the policies or positions of the US Government, the Department of Defense, or the US Air Force.