The Law of Cyberwar: A Case Study from the Future

Charles J. Dunlap, Jr. ©

By its very nature, much of the Anglo-Saxon legal tradition and, for that matter, the broader sphere of law of war, is not especially forward-looking. Reliance by judges on *precedent* illustrates that heritage.[1] This orientation towards the past has served the law well by providing carefully tempered analyses of real situations as opposed to speculation on imagined facts. It is from such fact-based analyses that the law produces the kind of seismic paradigm shifts that new developments occasionally require. This approach, however, is not an unqualified virtue. It usually results in a proclivity to wait for issues to arise in actual cases, to have them "ripen" so to speak, before definitively addressing them.

Against this backdrop the late twentieth century finds us well into what is popularly referred to as the "Information Age." This era is marked by scientific advances that are stimulating profound changes across the range of human endeavors. What differentiates this epoch from earlier ones is the unprecedented speed of the change. One need only consider that not so many years ago a computer sporting a hard disk with a capacity of 20 MB was considered state of the art; now systems with two hundred times that capacity are commonly found in computers marketed for home use. Furthermore, the phenomenal growth in the access to information brought about by the Internet is but one more indication of how quickly our weltenshanuung can change.

The velocity of this metamorphosis threatens to overcome the law's ability to accommodate change unless we engage in immediate, forward looking thinking. This is especially a concern with respect to legal issues associated with the military uses of these new technologies. Uniformed leaders all over the globe are urgently incorporating advanced computer, communications, and information systems into their weapons and forces because they believe that the way war is waged will be profoundly affected by innovative applications of the microchip. Indeed, the literature of security studies is infused with exchanges about what has become known as "The Revolution in Military Affairs" (RMA). Though there is no clear consensus as to precisely what that phrase means, it appears clear that at minimum it contemplates the integration of new technologies, and particularly information technologies, into military equipment, doctrine, organization and, ultimately, warfighting operations.[2] Many observers believe that the RMA will give the United States a virtually insurmountable military advantage for the foreseeable future.[3]

Among the many effects that the RMA may have on warfare, few are as intriguing as those related to information operations[4] and cyberwar.[5] Some enthusiasts contend that twenty-first century conflicts might be fought virtually bloodlessly in cyberspace. In a cyberwar scenario depicted in a 1995 *Time* magazine article, an Army officer conjured up a future crisis where a technician ensconced at a computer terminal in the United States could derail a distant aggressor without firing a shot simply by manipulating computer and communications systems.[6]

The purpose of this essay is to try to examine the kinds of legal questions that will soon confront (and in some instances, already have confronted) cyberwarriors. As this discussion proceeds it will become evident that the focus is more on identifying issues than resolving them. Along this line it is hoped that the foregoing emphasis on the rapidity of change and the importance of being proactive in dealing with that change does not imply that the current legal norms in fashioning solutions must be—or should be—abandoned. Quite to the contrary, the central thesis of this paper is that much existing law is applicable to cyberwar. In fact, the starting point for inquiry should always be the extent to which a new technology or means of warfare can find a context within the present legal framework of international law.

Nevertheless, the laws devotion to precedent complicates this task. Military leaders cannot afford to accommodate the laws deliberate but often plodding pace. They are under enormous pressure to aggressively apply the new technologies to the business of war. After all, analysts Ronald Haycock and Keith Neilson ominously warn that technology has permitted the division of mankind into ruler and ruled.[7] In the world of technology-intensive cyberwar, few military leaders will have the luxury of waiting for experientially-derived analyses. The absence of an actual case to study does not, however, necessarily foreclose the opportunity for productive legal interpretations.

In the February 1998 issue of *Wired* magazine, John Arquilla of the Naval Postgraduate School posits a fascinating and realistic tale of cyberwar entitled *The Great Cyberwar of 2002*.[8] In this fact-based fiction the U.S. is subject to a series of mysterious computer assaults. The nation fashions a variety of responses employing both high-tech electronic means as well as traditional, low-tech kinetic military methods. This short essay aims to identify some of the legal issues raised by the scenario and to provide vectors for possible solutions.

The issues

When Does War Begin?[9] In the opening paragraph of Arquillas story, the narrator says that he is sure that the great cyberwar began with the posting of a message (hacked onto several major news sites) from an organization calling itself People for a Free World (PFP). It demanded that the U.S. close all overseas military bases or face disruption and destruction of major infrastructure elements. When the U.S. fails to comply, cyberattacks against electrical grids, air traffic control computers, oil pipeline control mechanisms, and other infrastructure systems take place. As the plot develops, the U.S. launches traditional military counterattacks (using elite military units), as well as high-tech electronic cyberassaults against the presumed perpetrators.

Despite the fact that many cyberwarriors would readily characterize the PFP attacks as acts of war warranting a military response, the issue is not that simple. Consider that under the United Nations Charter adopted in 1945, the U.S. and other member nations agreed to eliminate the threat or use of force from international affairs. For example, under Article 2(3) of the Charter the signatories have agreed to settle their disputes—including many that might have once been considered acts of war—by "peaceful means." In other words, nations theoretically do not have the right to go to war absent UN sanction.

The Charter does, however, allow signatories to use force in certain limited circumstances. In addition to actions explicitly authorized by the Security Council, unilateral use of force is permitted in self-defense. Specifically, Article 51 of the Charter allows it to be used "if an *armed* attack occurs against a Member of the United Nations...." [Emphasis added.] The issue then is whether the use of a computer weapon (viruses, Trojan Horses, etc.) equates to an "armed" attack within the meaning of Article 51.

This is a good illustration of where technology is, perhaps, ahead of international law. Although electronic assaults can wreak havoc on advanced societies like that of the United States, such "attacks" do not automatically equate to an "armed" attack within the meaning of the UN Charter. As a general rule, "armed" attacks justifying an Article 51 response are largely limited to a significant assault using traditional kinds of kinetic weapons (e.g., bombs and bullets). In the 1986 decision in *Nicaragua v. United States*, for example, the International Court of Justice concluded that Nicaragua's support for rebels in various Central American countries did not justify the "armed" response (i.e., mining Nicaraguan harbors and other covert actions) by the United States.

Further support for the proposition that an "armed" attack warranting an Article 51 response does not include cyberassaults can be found by examining the Charter as a whole. In its outline of actions to be taken against recalcitrant nations, it seems to distinguish between acts constituting "armed" operations and lesser coercive measures. Article 41, for example, discusses "measures *not* involving the use of armed force" and cites as illustrations the "complete or partial interruption of *economic relations* and of rail, sea, air, postal, telegraphic, radio, and *other means of communication*...." [Emphasis added.]

Analogizing such tactics to a cyberassault that causes a "complete" or "partial interruption" of the electronic communications is not difficult. Thus, it appears that such methodologies probably do not *per se* constitute an "armed" attack under the Charter and Article 51 would very often *not* justify traditional military counterstrikes. Indeed, such military action, notwithstanding the electronic invasion, might constitute "aggression"—a serious allegation in the post-Nuremberg world. Some scholars argue, however, that the true meaning of "armed attack" under Article 51 relates to the intensity of the coercion imposed. Thus, it might be argued that where the economic damage caused by the electronic attack is of sufficient scale and scope, then the coercion equates to "armed attack" justifying an Article 51 response.

This appears to be the case in Arquillas scenario. The electronic assault in *The Great Cyberwar of 2002* causes not only enormous economic damage, but also the loss of life. Under these circumstances, that is, where there is clear evidence of reasonably foreseeable deaths directly attributable to the electronic "attack," it seems reasonable to equate a cyberassault with an "armed" attack as used in Article 51. Indeed, many experts would agree that where data manipulation directly results in significant destructive effects that are indistinguishable in any meaningful way from those caused by traditional (kinetic) weapons, such assaults constitute "armed attacks" for purposes of Article 51.

What about a lesser but still hostile manipulation of computer systems? Even if a particular cyberassault does not warrant a military response under Article 51, this does not mean that the U.S. would be without recourse. It could take the matter to the Security Council or other international fora for resolution. The Security Council could authorize

military force against an offending state even in the absence of an "armed attack." The requirement for an "armed attack" applies only to the authority to engage in self-defense pursuant to Article 51. Furthermore, just because an electronic attack does not sanction a traditional retaliatory military strike does not mean it is legal under international law. A whole range of international agreements may be violated—and a high-tech response might therefore be sustainable. An important study by Commander James N. Bond, USN, asserts that victims of an unlawful cyberattack that does not amount to a use of force as defined in international law, may still take proportional countermeasures that also do not amount to a use of force.[10] He maintains that one such response might be a "tit-for-tat" data manipulation.

In addition, the doctrine of state responsibility generally holds that every breach of international law creates a duty to pay for any loss or damage that results. Thus, even where a purely military response is not appropriate, the offending nation may still be held financially liable. The issue of state responsibility arises in *The Great Cyberwar of 2002* not only with respect to the aggressors, but also with regard to the U.S. itself when it is tricked into believing that the cyberattacks were launched from China and Russia. This proved to be erroneous, but only after an American counterstrike had wreaked havoc on the essential computer systems of those countries. This raises a key consideration for cyberwarriors, that is, the importance of positive identification of the perpetrator before launching a retaliatory response.

Status of Cyberwarriors. Of course, the question of when war begins presupposes a capacity to be a belligerent within the meaning of international law. In a legal sense, whether or not a nation is at war is largely dependent upon the status of the adversary. As a general proposition, war can only exist between states and not, for example, between the U.S. and the non-state actors like criminals and even criminal syndicates. A whole panoply of international agreements comes into play when *nations* are at war—the Geneva Conventions being just one example—that may affect the way a nation treats belligerents. For example, soldiers fighting in international armed conflicts cannot be punished for the harm they cause to military targets or for the deaths they inflict on other combatants so long as the law of war is otherwise observed.

As is to be expected, combatants in international conflicts can be attacked virtually anywhere, anytime. Civilian criminals, however, are not usually considered combatants, even during wartime. They are not, therefore, subject to attack *per se*, although deadly force can be used to halt their illicit activities in certain instances. Deadly force ordinarily also can be employed to take felony suspects into custody. Generally, destruction of the combatant forces of an enemy is a legitimate military aim; destruction of criminals is an option reserved to judicial processes, if at all.

Accordingly, when a cyberattack occurs during a period of putative peace, it is critically important for cyberwarriors to determine the *status* of the attacker as the parameters of the permissible response may differ radically. If the cyberassault is the product of state action, then the response is essentially governed by the law of war. If, however, the attack spawns from a criminal, or a consortium of criminals acting without state sanction, then the response is subject to the requirements of the criminal law. Military forces apprehending criminals—hackers or anybody else for that matter—must

defer to judicial prerequisites including such concepts as due process and the notion of the presumption of innocence—legal niceties not applicable to attacks on belligerent militaries in time of war.

The Great Cyberwar of 2002 presents a hybrid of these principles: criminal organizations in both South America and Asia ally themselves with bona fide states. Assuming the nature of the cyberassaults warrants characterization as elements of an international armed conflict, their commission during wartime may expand the legitimate range of actions that might be taken. As already indicated, under the law of war civilians—to include criminals—are normally considered noncombatants who are not subject to direct attack. Nonetheless, the law has always held that noncombatants immunity from damage and harm was predicated upon their obligation to abstain from hostile acts. If they took action against a party's armed forces, they automatically lost immunity.[11]

In this case it appears that the civilian criminals are engaged in hostile acts against the U.S. as surrogates for belligerent states. Under these circumstances *they should be characterized* as unlawful combatants under international law.[12] If captured, unlawful combatants can be tried and punished for their hostile actions, to include the same things for which uniformed combatants would be immune.[13] What is more is that while they are performing hostile acts they can be attacked on the same basis as regular military personnel. Although they should not be attacked when not actually performing hostile activities, they remain subject to being apprehended—using force if necessary—and tried for any violations of U.S. law they might have committed.

The criminal organizations used by the enemy are not the only civilians who might be characterized as unlawful combatants in *The Great Cyberwar of 2002*. The narrator and other cyberwarriors participating in the American counterattack are themselves civilians. This illustrates a long-held concern about the sophistication of the technologies needed for cyberwar. Specifically, they increasingly require civilian expertise for their operation and this blurs the distinction between civilian noncombatants and uniformed combatants.[14] While civilian technicians and contractors have long been associated with modern militaries, their continued status as noncombatants is premised on the idea that they confined themselves to support activities. A civilian technician, however, who helps *execute* a computerized counteroffensive cyber *attack* against an enemy system may well have gone beyond mere support.

In the U.S. the civilianization of what are—in high-tech, cyberwar terms—combatant functions appears to be accelerating. *Defense News* characterized the large numbers of civilian technicians required for the Army's digitized battlefield as surrogate warriors.[15] Likewise, the Air Force, probably unaware of the implications of its statement, has openly announced its intention to use civilians *operationally*. In *Global Engagement: A Vision for the 21st Century Air Force* the service states that combat operations in the 21st Century will broaden the definition of the future *operator*.[16] It goes on to state that: In the future, any military or civilian member who is experienced in the employment and doctrine of air and space power will be considered an operator.[17] It is very doubtful that many of these surrogate warriors are cognizant of their new status or comprehend the ramifications of it.

Since it is unlikely that military dependence on civilian cyberwar expertise will diminish any time soon, several writers suggest establishing a new type of part-time

military.[18] It would be composed of engineers, information specialists, and other technical experts who could be called into military service when necessary. Endowing civilians with military status would support recognition as lawful combatants under international law. While this approach would solve one technology-driven problem, it is not without complication because the military affiliation contemplated by the proponents would not require the technical experts to undergo all the rigors of military training.[19] In describing such an organization composed of information specialists, Brig. Gen. Bruce M. Lawlor, ARNG, argues that the well-paid innovators, intellectuals, and highly-skilled technicians most needed for cyberwar would not likely be impressed by the opportunity to wear hair high and tight or do pushups and two-mile runs.[20] Accordingly, he recommends that much of the military regimen be discarded.[21]

Decision makers need to be cautious, however, about abandoning much of the military regimen simply to indulge the predilections of civilian cyberwar experts. Military personnel are not just people in uniforms. There are instead, as Stephen Crane, the author of *Red Badge of Courage*, put it, a mysterious fraternity born out of smoke and the danger of death.[22] In his book, *Acts of War: The Behavior of Men in Battle*, Richard Holmes explains:

However much sociologists might argue that we live in an age of narrowing skill differentials, where many of the soldiers tasks are growing ever closer to those of his civilian contemporaries, it is an inescapable fact that the soldiers primary function, the use or threatened use of force, sets him apart from civilians...[T]he fact remains that someone who joins an army, is both crossing a well-defined border within the fabric of society, and becoming a member of an organization which, in the last analysis, may require him to kill or be killed.[23]

Importantly, Holmes argues that much of the military's regimen, even such mundane things as haircuts, has psychological importance beyond its obvious practical value. Many military requirements and rituals serve to acculturate an individual to the armed forces and to build the kind of unit cohesion and *esprit de corps* necessary to endure the enormous pressures of combat. The uncertainties and unpredictable dynamics of 21st century battlefields make it unwise to assume that technical experts will always be in situations that render unnecessary the kind of bonding and mental preparation that has sustained winning military organizations for centuries

Targets. The problem of determining who is and who is not a lawful combatant is not the only targeting-related issue arising in *The Great Cyberwar of 2002*. In both the cyber-attacks launched against the U.S., as well as in its counterattacks, the electronic infrastructure is targeted. In broad terms the law of war forbids attacks on civilian objects, including the infrastructure that supports noncombatants. Moreover, belligerents have an obligation to separate military targets from civilians objects in order to facilitate the latters protection.[24] In cyberwar this is an especially serious problem because most modern militaries depend upon the same electronic infrastructure as civilians use. Under these circumstances attacks on dual use systems are permissible so long as the adverse collateral effects on noncombatants are not excessive in relation to the direct and concrete military advantage anticipated.[25]

The U.S. should expect that its electronic infrastructure will be attacked because the U.S. armed forces relies heavily upon it. For example, more than 90 percent of the U.S.

military messages flow through commercial channels.[26] Professor Dan Kuehl of the National Defense University's School of Information Warfare and Strategy points out that this growing intermingling in the integrated information society of systems used and needed by both the military and civil sides of society...is making our national information infrastructure a viable, legal and ethical target in the case of conflict.[27]

Attacks against communications nodes and their related computer facilities do more than just inconvenience people in technologically-advanced societies. Such systems support essential emergency services and very often control critical parts of the infrastructure indispensable to civilians, especially in vulnerable urban areas. Similarly, cyberstrikes against electrical grids, designed to undermine a *military's* high-tech computer and communications capabilities, have profound and often unintended reverberating effects on noncombatants and their high-tech systems.[28]

What is missing from *The Great Cyberwar of 2002* scenario is any suggestion that the U.S. engaged in the proportionality analysis alluded to earlier. In other words, what the law of war requires is an analysis of the effects on noncombatants of actions such as closing down the electric grid before the attack is launched. If the effect on civilians is disproportionate vis-a-vis the direct and concrete military advantage anticipated, then the attack is impermissible. Too often it seems that cyberwarriors assume the issues about civilian casualties are avoided because the *immediate* casualties of an electronic assault may be few.[29] It is the less visible long term, secondary effects of technology loss that must be evaluated as well.

Attacks on dual-use systems need not, however, be foregone. Rather, what is needed is a firm grasp of the long-term, *indirect* impact upon noncombatants *prior* to the authorization of an attack as well as an ability to quantify the expected military advantage. Clearly, an enhanced intelligence architecture is necessary to provide the right kind of data to conduct the more probing proportionality calculation these new technologies require.[30] One way of analyzing the data that an enhanced intelligence system might provide would be to employ the new modeling and simulation techniques now becoming available. For example, using data drawn from Joint Resource Assessment Data Base, U.S. Strategic Command's Strategic War Planning System (SWPS), can project the expected numbers of killed and injured when a given nuclear weapon is delivered by a designated platform in a certain fashion on the selected target.[31] Similar systems could be developed to analyze the effects of cyberattacks on high-tech networks.

However, modeling and simulation themselves present significant issues. Specifically, are military leaders legally or morally *obliged* to follow the model? Suppose, for example, that a decision maker chooses a course of action that the model shows will result in greater noncombatant casualties than another available option. Since the legal and moral duty is to take all feasible precautions to avoid noncombatant casualties,[32] if a computer calculates that a certain method of attack among several options most minimizes noncombatant loses, does that automatically preclude consideration of other options? If a commander selects another option, has he failed to do everything feasible to avoid noncombatant losses?

As technology progresses one might fairly expect the fidelity of the models to improve,[33] but it is not yet clear that they can *ever* substitute for the judgment of the commander in the performance of the warfighting *art*. The linear, mathematical nature of

computer processes may never be able to replicate the nonlinear and often unquantifiable logic of war.[34] The history of human conflict is littered with examples of how military forces achieved results that no algorithm would have predicted.[35] Still, in a world that increasingly considers reports provided by an electronic brain innately more authoritative than human-derived analyses, it may well behoove cyberwarriors in future conflicts to somehow capture the essence of their rationale when they select a computer-produced option that on its face seems to be more casualty-intensive than another course of action assessed by the same source.

Cyberweapons and Cybotog. Closely related to the targeting issues raised by cyberwar are questions concerning the cyberweaponry itself. Specifically, the law of war allows the employment of only those means or method of warfare that can effectively discriminate between military personnel and civilian noncombatants.[36] In *The Great Cyberwar of 2002* all of the adversaries use a variety of viruses and other high-tech means to incapacitate various computer systems. It is unclear, however, whether once released these various electronic agents can realistically be confined to military objectives. If there is no practical means of ensuring that their nefarious effects can be reasonably limited to bona fide targets, their use may be barred. In a variety of ways, a computer virus loosed on a technology-dependent high-tech society may be as devastating to noncombatants as many of their biological namesakes.

Other means of waging war in the information age deserve re-consideration in the context of the information age. Near the end of *The Great Cyberwar of 2002* the U.S. president authorizes a cybotog campaign against North Korea designed to collapse its regime and reunify the peninsula.[37] The precise means are not discussed, but it is presumed that some kind of sophisticated technology-aided psychological campaign is employed. There is nothing necessarily wrong with doing so. Historically, propaganda campaigns aimed at toppling adversary governments are considered legitimate means of waging war.[38]

Emerging information technologies give cyberwarriors powerful new tools to conduct such operations. Among them is the ability to manufacture realistic but false television images.[39] Thomas Czerwinski, then a professor at the School of Information Warfare of the National Defense University, suggests how such technologies might be used when he 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?[40]

When the government undermined by this kind of cyberwar operation is a totalitarian one, there is little concern, at least during wartime.[41] But this norm may need re-examination when the government affected is a democratic one. Among other things, it needs to be reconciled with a primary component of U.S. national security policy: the promotion of democracy. While no one would dispute that the improper *actions* of the leaders of any enemy 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, the author of the classic treatise, *Just and Unjust War*, asserts that war aims legitimately reach to the destruction or defeat, demobilization, and (partial) disarming of the aggressors 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.*[42] Surely, a democratic

government is not the kind of extreme case that Walzer exempts. Thus, decision makers may wish to develop policies that restrain information warriors from engaging in tactics that damage the democratic process. Democracy has an intrinsic human value even when it produces governments whose actions lead to war.

Parenthetically, there is another aspect of these cyberwar strategies that deserves mention. Because of their enormous potential to affect political processes in democracies—including our own—it may be wise, in the interest of civil-military relations, to place the organizational responsibility for their employment under the control of a civilian entity. There is precedent for this in the control of nuclear weapons by the Department of Energy as provided by the Atomic Energy Act.[43]

Conclusion

This brief discussion has by no means enumerated all of the possible legal issues associated with *The Great Cyberwar of 2002*. Rather, it is meant to illustrate how the existing law of war might apply to cyberwar notwithstanding the absence of a portfolio of supporting precedents. In most instances the application was direct and reasonable. The underlying principles of the traditional law of war are usually just as applicable to electronic conflicts as to wars using principally kinetic means.

That said, there are certain areas of the law applicable to cyberwar that need attention: as indicated previously, an internationally accepted definition of the kinds of electronic attacks that equate to armed attacks within the meaning of Article 51 of the U.N. Charter is a necessary clarification. Clear guidance as to what would support acts of self-defense—to include traditional military action—would facilitate planning and perhaps even serve to deter potential adversaries. One obvious method of qualifying cyberassaults as "armed attacks" is to simply define electronic methodologies as "weapons." In this respect a 1974 UN resolution defined the "use of *any* weapons by a State against the territory of another State" as "aggression." The United States, however, should approach such proposals with caution. They may result in unintended limitations when applied to the range of emerging cyberwar technologies. While the U.S. has many vulnerabilities to cyberassault, it also has great potential capability.

The law of cyberwar may develop other ways as well in the 21st century. At the conclusion of *The Great Cyberwar of 2002* the international community agrees to a ban on information warfare as well as to a pledge of no first use of cyberweapons. The story's narrator, however, is doubtful about the efficacy of the agreements. The story suggests that he believes they would be difficult to enforce and would not, in any event, have much effect on rogues, terrorists, and criminal organizations that started the fictional war in the first place.

Even if one assumes the cynicism that the narrator expresses has at least facial validity, that is not a reason to discount efforts to look for legal avenues of restraining cyberwar. The fact that rogues, terrorists, and criminals ignore international law does not mean it has no use. Nations, by and large, *do* honor it for a variety of reasons. Moreover, it is too easy to forget that many of the same arguments were made with respect to nuclear weapons. Yet today we see an extensive international legal regime that, while not completely successful, has at least made progress towards the dream of a nuclear free world.

In the meantime, cyberwarriors should ensure that their warfighting complies with existing international law. Simply because a method of warfare is new and different does

not mean that it is unregulated by the law of war. For U.S. forces, as well as those of other democracies, honoring the rule of law is necessary to achieve the political goals of war. It would be a great mistake for cyberwarriors to underestimate how the fact and perception of lawfulness can materially affect the public support that military operations conducted by democracies require. 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.*[44]

Thus, for very clear *military* reasons observance of the law in cyberwar is just as important as it is during any other military operation. In the final analysis, the law of cyberwar is not so different from the traditional law of war. Nor is cyberwar likely to induce change so dramatic so as to render irrelevant the many years of precedent and other legal developments produced by centuries of more conventional forms of warfare. Law may not be able to prevent human conflict but it can make it more humane—something which hastens war termination and the restoration of peace. Cyberwarriors need to remember that *how* they fight the war may well determine the kind of peace that emerges.

Endnotes

[1] The law of war or law of armed conflict (LOAC) as it is often characterized, 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.
See Captain Robert G. Hanseman, USAF, The Realities and Legalities of Information Warfare, 42 A.F. L. Rev. 173, 189.

[2] Precedent is defined in the law as [a]n adjudged case or decision of a court of justice considered as furnishing an example or authority for an identical or similar case afterwards arising or a similar question of law. *Blacks Law Dictionary* (Henry Campbell Black, ed., rev. 4th ed., 1968), at 1340.

[3] For a discussions of the revolution in military affairs in the information age see generally, Select Enemy. Delete., *The Economist*, March 8, 1997, at 21; Eliot A. Cohen, A Revolution in Warfare, *Foreign Affairs*, March/April 1996, at 37; Andrew F. Krepinevich, Cavalry to Computers: The Pattern of Military Revolutions, *The National Interest*, Fall 1994, at 30; and James R. Fitzsimonds and Jan M. Van Tol, Revolutions in Military Affairs, *Joint Force Quarterly*, Spring, 1994, at 24.

[4] The Future of Warfare, *The Economist*, March 8, 1997, at 15.

[5] There are many possible definitions of information operations but a common official definition is that used by the Air Force, that is, actions taken to gain, exploit, defend, or attack information and information systems.) *Air Force Doctrine Document 1*, Air Force Basic Doctrine (September 1997), at 44 (hereinafter AFDD-1). This definition is almost identical to that once used by the Air Force to describe information warfare. See Captain Robert G. Hanseman, supra note 2, at 176 citing USAF Fact Sheet 95-20 (Nov. 1995

[6] Cyberwar suggests a form of warfare more holistic, strategic, and manipulative of information in its concept than the information operations definition set forth in note 6 supra. AFDD-1 notes the following: "In describing information operations, it is important to differentiate between information in war and information warfare. The second element, information warfare, involves

such diverse activities as psychological warfare, military deception, electronic combat, and both physical and cyber attack." AFDD-1, id. For an excellent cyberwar scenario, see John Arquilla, The Great Cyberwar of 2002, *Wired*, February 1998, at 122.

[7] He visualized the foe's phone system brought down by a computer virus, logic bombs ravaging the transportation network, false orders confusing the adversary military, the opponents television broadcasts jammed with propaganda messages, and the enemy leaders bank account electronically zeroed out. All of this is expected to cause the adversary to give up. See Douglas Waller, Onward Cyber Soldiers, *Time*, August 21, 1995, at 38.

[8] Id., at xii.

[9] John Arquilla, The Great Cyberwar of 2002, *Wired*, February 1998, at 122.

[10] Elements of this section were taken from the authors article entitled Cyberattack! Are We at War?, *Journal of the National Computer Security Association (NCSA News)*, November 1996, at 18.

[11] See generally, Commander James N. Bond, USN, Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2 (4), Advanced Research Project, Center for Naval Warfare, Naval War College, 14 June 1996 (unpublished manuscript on file with the author).

[12] Paul Kennedy and George J. Andreopoulos, The Laws of War: Some Concluding Reflections, in *The Laws of War: Constraints on Warfare in the Western World* 215 (Michael Howard, George J. Andreopoulos, and Mark L. Shulman, eds., 1994).

[13] Department of the Air Force Pamphlet 110-31, International Law The Conduct of Armed Conflict and Air Operations (19 November 1976) at paragraph 3-3 [Hereinafter referred to as AFP 110-31] provides: An unlawful combatant is an individual who is not authorized to take a direct part in hostilities but does. The term is frequently used also to refer to otherwise privileged combatants who do not comply with requirements of mode of dress, or noncombatants in the armed forces who improperly use their protected status as a shield to engage in hostilities... Unlawful combatants are a proper object of attack while engaging as combatants...If captured, they may be tried and punished.

Id., See also Lt. Colonel Robert W. Gehring, Loss of Civilian Protections Under the Fourth Geneva Convention and Protocol I, 90 *Mil. L. Rev. 49* (1980).

[14] Unlawful combatants are not ordinarily considered war criminals. Rather, they would be subject to prosecution under the domestic law of capturing belligerent, much as out-of-uniform saboteurs would be. During World War II, for example, the United States captured eight German saboteurs and executed six. See *American Heritage New History of World War II* 276 (Rev. and updated by Stephen E. Ambrose based on the original text by C. L. Sulzberger, 1997).

[15] Compare AFP 110-31, supra note 14 at paragraph 3-5.

[16] See Bryan Bender, Defense Contractors Quickly Becoming Surrogate Warriors, *Defense Daily*, March 28, 1997, at 490.

[17] United States Air Force, *Global Engagement: A Vision for the 21st Century Air Force* (1997), at 7.

[18] Id., at 19.

[19] See Stephen Bryen, New Era of Warfare Demands Technology Reserve Force, *Defense News*, March 17-23, 1997, at 27; and Brig Gen. Bruce M. Lawlor, ARNG, Information Corps, *Armed Forces Journal International*, January 1998, at 26, 28.

[20] Id.

[21] Lawlor, supra note 20.

[22] Id.

[23] As quoted in Richard Holmes, *Acts of War: The Behavior of Men in Combat* (1985), at 31.

[24] Id.

[25] *W. Hays Parks, Air War and the Law of War, 32 A.F. L. Rev.* 1, 168 (1990).

[26] Essentially, the concept of proportionality requires commanders to refrain from attacks when it may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian

objects or combination thereof, which would be excessive in relation to the direct and concrete military advantage anticipated. See AFP 110-31 supra note 14, at paragraph 5-3c(1)(b)(I)(c).

[27] John T. Correll, Warfare in the Information Age, *Air Force Magazine*, December 1996, at 3.

[28] Daniel Kuehl, The Ethics of Information Warfare and Statecraft, Paper presented at InfoWARcon 96 (Washington, D.C., September 1996) (on file with author).

[29] 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).

[30] See note 27 supra.

[31] See Winn Schwartau, The Ethics of Civil Defense and Information Warfare, *Journal of the National Computer Security Association* (NCSA News), June 1997, at 15, 16-17.

[32] See note 27 supra.

[33] The system uses terms that have specific definitions and this affects the evaluation. For example, casualties are defined as the estimated number of people who die or receive injuries that require medical treatment [or] die due to short term effects (6 months) of nuclear detonations. Population at Risk is defined as the total civilian population in danger of dying, independent of shelter, from short term (6 months) effects of nuclear detonations. See Memorandum, Acronyms/Definitions Used in SIOP Analysis (U), USSTRATCOM Plans and Policy Directorate, Force Assessment Branch (April 1997) (on file with author).

[34] See AFP 110-31, supra note14, at paragraph 5-3c(1)(b)(I)(c).

[35] See generally, Paul R. Camacho, Further Development in the Construction of Political Action Expert Systems Software: Fuzzy Logic Techniques on Social Science Variables, a presentation for the Biennial International Conference of the Inter-University Seminar on Armed Forces and Society, Baltimore, MD, October 24-26, 1997 (unpublished paper on file with author).

[36] War is typically nonlinear, meaning the smallest effects can have unpredicted, disproportionate consequences. See Jeffrey McKitrick, James Blackwell, Fred Littlepage, George Kraus, Richard Blanchfield and Dale Hill, Revolution in Military Affairs, in *Battlefield of the Future* (Air University, 1995). See also Glenn E. James, *Chaos Theory: The Essentials for Military Applications* 57-95 (Newport Paper No. 10, Naval War College, 1996) (discussing the limitations of computer modeling).

[37] See, Robert N. Ellithorpe, Warfare in Transition? American Military Culture Prepares for the Information Age, a presentation for the Biennial International Conference of the Inter-University Seminar on Armed Forces and Society, Baltimore, MD, October 24-26, 1997, at 18 (copy on file with the author). (History has demonstrated the fatal error of military decisions based on the use of scientific and technical analysis at the expense of understanding the warfighting art.).

[38] See AFP 110-31, note 14 supra, at paragraph 6-3c.

[39] Though beyond the scope of this paper, it is not clear that action during peacetime to topple any regime is consistent with the underlying premise of the UN Charter calling for non-interference with the internal affairs of member nations.

[40] See e.g., Department of the *Army Field Manual 27-10* (July 1956) at paragraph 49.

[41] See Dennis Brack, Do Photos Lie? *Proceedings*, August 1996, at 47.

[42] As quoted by Peter Grier, Information Warfare, *Air Force Magazine*, March 1995, at 35.

[43] See note 40, supra.

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

Colonel Dunlap is Staff Judge Advocate of U.S. Strategic Command. The views and opinions he presents are his alone and do not necessarily represent those of the Department of Defense or any of its components. Copyright 1998, Charles J. Dunlap, Jr.

The author has discussed elements of this essay in a previous paper entitled Technology and the Twenty-first Century Battlefield: Re-complicating Moral Life for the Statesman and the Soldier, presented on 6 February 1998 in Annapolis, MD, to the Ethics and the Future of Conflict Working Group meeting sponsored by the Carnegie Council on Ethics and International Affairs.