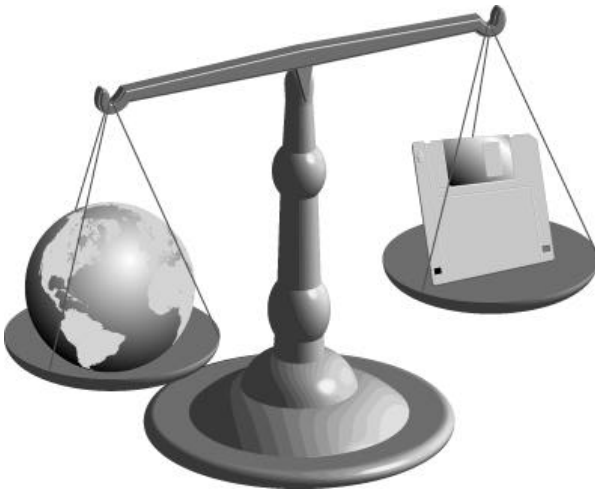
The International Legal Implications of Information Warfare

MAJ RICHARD W. ALDRICH, USAF*



Because exploiting [information systems] will readily cross international borders, we must be cognizant of what the law allows and will not allow. We must have good legal advice as we get into this.

—Gen Ronald R. Fogleman
Chief of Staff of the Air Force

IN HIS REMARKS, quoted in *Computerworld* in June 1995, General Fogleman was speaking of "information warfare." Information warfare is believed by many to be the means by which the next "big" war will be fought and, more importantly, the means by which future wars will be won. The term itself is enigmatic, embracing concepts as old as war itself and as new as the latest technology. The recent meteoric rise in prominence of the concept is inextricably linked to the dramatic advances in communications technology and information systems, specifically the computer.

> Some scientists suggest that the most important invention is not "wireless communication, flying, the internal combustion engine or the atomic bomb but the digital computer;" for, while the others may be a threat to our environment, our privacy or our lives, none of them can threaten our image of ourselves in the way the computer can.[1]

Nor may any of them affect how wars are fought as much. The futurists Alvin and Heidi Toffler,

*Special thanks to Lt Col Bill Schmidt and C1C Chuck McLean for reviewing this paper. The views expressed are those of the author and do not necessarily reflect those of the INSS, the Air Force Academy, the United States Air Force, or the Department of Defense.

authors of *The Third Wave* and *War and Anti-War,* claim we have entered a new era, an information age they refer to as the "third wave" to differentiate it from the agrarian and industrial periods of the first and second waves, respectively. In the third wave, information ascends to become the most important resource and as such becomes not only an end of war, but also one of the significant means of winning wars.

[Exemplified by AWACS, ground satellite communications stations, and orbital communications satellites,] "the American military is also the most information-dependent force in the world. . . ." [It] is also the most networked force in the world, a combination which, absent adequate defenses, makes the American military extremely vulnerable to information attacks.

Many scoff at the idea as so much hype. Perhaps some is overhyped, but it is important to realize that

> the American military is the most information-dependent force in the world. It uses computers to help design weapons, guide missiles, pay soldiers, manage medical supplies, write memos, control radio networks, train tank crews, mobilize reservists, issue press releases, find spare parts and even suggest tactics to combat commanders.[2]

The American military is also the most networked force in the world, a combination which, absent adequate defenses, makes the American military extremely vulnerable to information attacks. The country's heavy civilian reliance on computers in communications, air traffic control, banking, and the stock exchanges has prompted one who should know, National Security Agency director Vice Adm John McConnell, to comment that "we're more vulnerable than any nation on earth."[3] The Joint Security Commission has characterized American vulnerability to information war, or infowar, as "the major security challenge of this decade and possibly the next century."[4] Individuals, terrorist groups, or foreign countries capable of penetrating the military's information systems could wreak havoc on our national defense.

Some say the war has already begun. Robert Ayers of the Defense Information Systems Agency (DISA) has concluded that Department of Defense (DOD) computers were broken into by unknown persons in excess of 300,000 times in 1994. Indeed, DISA itself tried to test the military's vulnerabilities by hacking into 8,932 DOD computers. DISA successfully gained control of 88 percent of them, using only "front door" attacks. Even more discouraging is the fact that only 4 percent of those hacked into even knew they had been victimized, and, shockingly, only 0.2 percent reported it.[5]

How, then, does the law of war and other international law limit this new form of warfare, if at all? To answer that question, this article first explores the definition of the term *information warfare,* then discusses the appropriateness of applying the law of war to information warfare techniques.

Definitions

How the law of war and international treaties proscribe the scope and use of information warfare hinges largely on how information warfare is defined. Unfortunately, the definitions are multifarious. Indeed, there are even various terms used in lieu of or in addition to the term, including *infowar, information operations, netwar, command and control counterwar* (C2W), *third-wave war, knowledge war,* and *cyberwar*.[6] The term *information*-based warfare is sometimes used to denote a subset of information warfare, but can also describe a precursor of a narrower concept of infowar:

> Information-based warfare is an approach to armed conflict focusing on the management and use of

> information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based warfare is both offensive and defensive in nature—ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets.[7]

Some also distinguish information-age *warfare* from *information warfare.* The former term "uses information technology as a tool to impart . . . combat operations with unprecedented economies of time and force,"[8] while the latter "views information itself as a separate realm, potent weapon and lucrative target."9

Information assurance is most often used by nonmilitary individuals and organizations to denote only the defensive aspect of information warfare, though many in the corporate community employ the term *information warfare* interchangeably.

Winn Schwartau, author of the book *Information Warfare: Chaos on the Electronic Superhighway,* defines *information warfare* as "an electronic conflict in which information is a strategic asset worthy of conquest or destruction."[10] He also defines three classes of information warfare: class 1 is *personal information* warfare, class 2 is *corporate information* warfare, and class 3 is *global information warfare.* The Computer Security Institute defines it as being

> distinct from "computer crime" because it implies an aggressive act on the part of one adversary—whether an individual, a competing organization or a rival government—against another in an ongoing struggle for hegemony in the marketplace or the political arena.[11]

It goes on to distinguish information warfare from "information gathering" by noting that the former carries with it the threat of interrupted operations and destroyed assets in addition to the loss of secrets normally associated with another's information gathering.[12]

Arguably, denying all information-transfer media and disrupting or destroying every transmission goes beyond a military objective by incapacitating the entire civilian populace as well.

According to the *Washington Post*, "the Pentagon formally defines infowar as the effort to seize control of electronic information systems during a conflict."[13] In point of fact, this assessment of the Pentagon's definition of information warfare seems far too narrow. Indeed, some in the Pentagon have defined information warfare so broadly as to encompass virtually the full spectrum of warfare activities. In a publication recently released by the Air Force entitled *Cornerstones of Information Warfare*, information warfare is defined as "any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[14] It emphasizes that under this definition information warfare is dependent only on the nature of the action, not the means by which it is accomplished. Thus, the conventional bombing of a computer center is information warfare under this definition, but it would not be under definitions offered by Schwartau and others. The National Defense University defines it as "the use of information and information systems as weapons in a conflict where information and information systems are the targets." This would presumably include the wartime use of propaganda and psychological operations (psyop).

However the term is defined, its very name may make matters slightly more complicated from a legal perspective. Under the broadest definitions, information warfare would be an activity engaged in both during peacetime and conflict. Calling a peacetime activity "information

warfare" may unnecessarily suggest the applicability of the laws of war or the appropriateness of defensive measures. It was perhaps for this reason that the United States Army has referred instead to the concept as "information operations." In spite of this, the term information warfare seems already too entrenched in the American vocabulary to change anytime soon. And obviously the vocabulary does not drive the law. Calling a pencil a nuclear weapon, for instance, does not make it one, but it would certainly introduce unnecessary confusion if a foreign country learned that the Pentagon was purchasing one million of these new "nuclear weapons."

Who is a "combatant" in the information age? If teenage hackers in the enemy's country unilaterally decide to aid their government by creating havoc through their use of computers, are they now fair game for attack by the opposition?

The Law of Armed Conflict

Despite the lack of a universally agreed upon definition of information warfare, this article concentrates on that aspect of information warfare dealing with the use of information systems for offensive or defensive purposes. Conventional attacks against information systems can largely be dealt with using traditional law of armed conflict (LOAC) constructs to assess military necessity, proportionality, collateral damage, and the like. It is the use of nontraditional "information weapons" that raises the most interesting questions under current law and that will be the focus of this article.

Armed Conflict

The *law of armed conflict* is also variously referred to as the *law of war*, though the former term seems more popular as nation-states today rarely declare war but frequently involve themselves in armed conflicts. The law of armed conflict necessarily applies whenever two nation-states are involved in an armed conflict.[15] But what is "armed conflict"? The expression "international armed conflict" is not defined in the Geneva Conventions or elsewhere in international law, but several commentators would consider that, at a minimum, it would apply "wherever regular armed forces engage the regular armed forces of a foreign state or enter the territory of a foreign state without permission."[16] "Engage" appears to envision a physical confrontation, and "enter[ing] the territory of a foreign state" envisions a physical entry, thus in both cases skirting the concerns raised by information attacks. Some may find it less problematic, characterizing an information attack as force if there is a physical manifestation such as an explosion. But this comprises only a fraction of the potential manifestations of information attacks. "Armed conflict," as presently understood, seems far less likely to be applied to the simple manipulation of bits inside a computer, although this may soon change since the nefarious manipulation of bits could, in some cases, already cause significantly more harm than could a bomb.

Armed conflict under shared Article 2 of the Geneva Conventions was specifically chosen over the term war because of its broader scope, but its scope in 1949 could hardly have envisioned the information warfare conflicts possible today. The commentator Jean C. Pictet concluded that "any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war."[17] This only shifts the question to what constitutes "intervention," but again the thrust seems to be one of physical confrontation. If an information attack does not fit the definition of an "armed conflict,"

A SATCOM facility in Southwest Asia during Desert Shield/Storm (right). An AWACS crew during Desert Shield/Storm (below right). A NATO III satellite (below left).

then many if not all of the laws of armed conflict are not even applicable.

Cyberspace versus Land, Sea, Air, and Space

The Geneva and Hague Conventions both deal, by their titles, with the issues of laws of war on land or at sea. Even the 1977 protocols to update the Geneva Conventions continued this connection to the land or sea, while other law of war treaties dealt with the air and space. This corporeal division worked well for first- and second-*wave* societies dealing with agrarian and industrial matters, but falls short in proscribing conduct in the information age. Information warfare takes place in what has come to be known as cyberspace, an ethereal place that does not neatly fit into the land, sea, air, space dichotomy.[18] Information warfare involves conduct and effects that transcend national boundaries and render such distinctions superfluous.

Further actions in cyberspace do not come cloaked in military garb. The information attack against a military computer could be the work of a curious teenager down the street, the work of terrorists in a nearby country, or the work of a belligerent government halfway around the world. One cannot always trace the source of the action, and even when the action can be traced back, it may lead only to an anonymous remailer. When an intercontinental ballistic missile (ICBM) is launched from Russia, it is a fairly clear signal of the start of an armed conflict. Even if an information attack can be traced to Russia, it is unclear whether the teenager, the terrorist group, or agents of the government are at the keyboard. Some may say that this is little different from the anonymous terrorist attacks occasionally suffered by military personnel and installations. The killing of American soldiers in German discos is a prominent example. In such a case, the United States merely relied on other sources of intelligence to fill in the ambiguities. In the German disco case, intelligence sources were able to sufficiently point the finger at Libya to justify military air strikes against it. Perhaps the same can be done in the area of information attacks, though it is interesting to note that the State Department's antiterrorism unit narrowly defines terrorism to be only politically motivated *physical* attacks. Thus, information attacks would not generally even fit within the definition of terrorism.

Basic Principles

There are three basic principles central to the law of armed conflict. It is instructive to analyze the applicability of LOAC to information warfare by analyzing these basic principles.

Principle of Military Necessity. The first principle of LOAC is that of military necessity. Briefly, it "permits the application of only that degree of regulated force, not otherwise prohibited by the laws of war, required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources."19 Professor Francis Lieber defines it as "those measures which are indispensable for securing the ends of war and which are lawful according to the modern law and usages of war."20

This first principle would seem to pose few hurdles for information warfare. It is unclear what exactly is the scope of the term *regulated force*, but this term could pose some problems with the employment of certain types of computer viruses. Viruses are often listed among the available "information weapons." Viruses, worms, Trojan horses, or logic bombs are all programs or sections of computer code that are designed to wreak havoc on a recipient's computer. They can be designed to trigger upon the occurrence of a certain event or to activate randomly. Randomly triggered viruses, worms, Trojan horses, and logic bombs may not properly fit the definition of the use of regulated force.

The negative definition encompassed in the concept of military necessity, permitting that which is not otherwise prohibited by the laws of war, currently works to the advantage of information war advocates, since much of the law of war was set down prior to any conceptualization of information weaponry and information warfare tactics. This relative void thus does little to impede this new form of war, though as will be seen

below, some international treaties may provide some barriers.

The stipulation that the submission of the enemy be accomplished with the least expenditure of life, time, and physical resources also favors information warfare, since it is largely viewed as a bloodless type of warfare. Information attacks may take little time, as they can potentially travel at the speed of light and they generally are aimed at disrupting information systems. Therefore, information warfare attacks are less likely to result in the loss of physical resources or lives, though some attacks do aim to physically destroy chips internal to a computer to cease its operation.

While not much has yet been written on how information warfare will be conducted, Col Owen E. Jensen recently wrote an article "for those seeking a few fundamental principles to guide them in applying information warfare to specific scenarios."[21] In his article, he emphasizes the importance of the Principle of Decapitation, which he describes as follows:

> Cut or deny *all* the enemy's information-transfer media—telephone, radio frequencies (RF), cable, and other means of transmission. Sever the nervous system. Deny, disrupt, degrade, or destroy *every* transmission.
>
> Stop all "gray system" access. Close off to the enemy all third-party communications satellites (COMSAT), whether they belong to international consortia or to commercial enterprises or are assets of uninvolved nations. (Emphasis added) [22]

The all-inclusive nature of this principle raises several legal issues: (1) its scope probably exceeds the bounds of military necessity, (2) it probably violates the treaties concerning international telecommunications satellites (INTELSAT) and international maritime satellites (INMARSAT), and (3) it probably violates the treaty concerning neutrals. Only the first issue will be addressed here. The latter two will be addressed in the appropriate sections below.

*Again, the principle of military necessity allo*ws only for the application of that degree of regulated force required for the partial or complete submission of the enemy with the least expenditure of life, time, and physical resources. Arguably, denying all information-transfer media and disrupting or destroying every transmission goes beyond a military objective by incapacitating the entire civilian populace as well. Taking out all information-transfer media would bring down a country's stock market, banking system, air traffic control, emergency dispatches, and more. This would almost certainly result in the loss of civilian lives and may well be deemed disproportionate to the military objective. The difficulty in the information age, however, comes in drawing the line. In the United States, for example, over 95 percent of military communications traverse civilian lines. The use of fiber optics and packet switching makes it virtually impossible to take out only the military communications. Nevertheless, taking out the entire civilian system would seem too blunt an approach under the law of armed conflict. Taking out military communications centers and military radio frequencies and manipulating military messages so as to create confusion and render even good messages suspect would be a far more defensible position. If the enemy's military shifted to civilian communications centers and civilian frequencies in response, it would now be more clearly legal to attack them, even with the consequent collateral effects to civilians.

The Air Force's *Cornerstones of Information* Warfare notes a troubling asymmetry between offensive and defensive actions under information warfare:

> The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of information warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military informtion functions. There are many information functions critical to our national security that lie outside the military's defensive purview.[23]

Indeed, as previously noted, reliable sources estimate over 95 percent of military communications traffic over commercial communications systems.[24]

The issue raises another point, though, and that is who is a "combatant" in the in formation age? If teenage hackers in the enemy's country uni-

laterally decide to aid their government by creating havoc through their use of computers, are they now fair game for attack by the opposition? If civilian radio and television stations unwittingly broadcast coded messages to the enemy's troops, can they be attacked?

Principle of Humanity. The second basic principle is the principle of humanity. Its aim is to prohibit "the employment of any kind or degree of force not necessary for the purposes of war that is for the partial or complete submission of the enemy with the least possible expenditure of life, time and physical resources." [25]

The law of land warfare forbade the employment of "arms, projectiles, or material calculated to cause unnecessary suffering." Included as examples were lances with barbed heads, irregularly shaped bullets, bullets with the hard-shell heads filed off or bullets dipped in an inflammatory substance, and projectiles filled with glass. [26] The 1981 Convention on the Prohibition or Restriction on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects added weapons that resulted in nondetectable fragments in the body, field mines, booby traps, and incendiary weapons. [27] These proscriptions are all very specific and fail to form any cohesive framework from which logical extensions could be made. Thus, while bullets dipped in an inflammatory substance are banned, the United States has long claimed that nuclear weapons are not excluded per se under the principle of humanity. Additionally, all of the specific weapons listed are rudimentary weapons of an older era with little real connection to any of the weapons envisioned for use in information warfare. With such specificity and incongruity, it would be difficult to automatically exclude any information weapon, though the overarching ban on weapons calculated to cause unnecessary suffering may provide a hazy boundary.

The issue of neutrals may pose interesting legal issues under information warfare.

Herein lies another problem with the language employed in information warfare: the theoretical talk of certain types of computer programs as "weapons." The law of armed conflict requires any nation desiring to implement a new type of weapon to make a determination prior to its use regarding its compliance with the principle of humanity. [28] If one calls up a computer program, whether it be a virus, worm, logic bomb, or something else a "weapon," this may unwittingly trigger a required review. Certainly, computer programs in and of themselves have not previously been considered weapons in the international community, though their effects may have some striking parallels with conventional weapons in some uses.

Some "weapon" use may also be constrained by domestic law even in its international application. For instance, if in the course of employing international infowar data-collection techniques, "United States persons" become subjects, Executive Order 12333 may apply. In pertinent part, it states:

> 2.4 *Collection Techniques.* Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.

> 2.5 *Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.[29]

While domestic law is beyond the scope of this paper, it is worth emphasizing that even operations taking place entirely in a foreign country or countries may be constrained not only by the foreign country's law and international law, but by domestic law as well. This is not peculiar to information warfare; rather, it applies across the board.

Other data-collection techniques will likely be treated in the same way that espionage is currently treated. That is, while it is not prohibited by the laws of armed conflict, it is punishable by the laws of an enemy state if the enemy can capture the spy and exercise its jurisdiction over him or her. Infowar roles that may fit this bill are "sniffing," "dumpster diving," and "cracking." Sniffing generally entails the use of software to record the first several characters of a telnet session. This information generally includes the username, Internet Protocol (IP) address, and password—enough information for the sniffer to breach security and/or pose as the sniffee. Dumpster diving, while oftentimes listed as an information warfare technique, is nothing more than the low-tech search through the trash of the opposition in search of user IDs, passwords, and the like to allow infiltration of the enemy's information systems. Cracking is the more sophisticated use of computers to access or create back doors to the enemy's computer systems. It may also involve setting up Trojan horses, circumventing firewalls, or attempting to obtain root access.[30] In addition to or in lieu of espionage laws, some countries may also have computer crime laws under which such conduct may be prosecuted.

Of particular note in this area is the United Kingdom's (UK) Computer Misuse Act. The act broadly proscribes many actions that would be included within the sniffing and cracking functions described above:

> (1) A person is guilty of an offence if—
>
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
>
> (b) the access he intends to secure is unauthorised; and
>
> (c) he knows at the time when he causes the computer to perform the function that that is the case.[31]

Of even greater significance, however, is the fact that the act purports to apply extraterritorially, as long as any significant link with British jurisdiction exists.[32] A significant link includes any access of a computer in the UK.[33] Based on the fact that the Internet is designed to withstand nuclear attack by sending message packets through any working node, the scope of this act is perhaps broader than its language would at first appear. Thus, if a French operative were to attempt to make a nefarious entry into a US Department of Defense computer and the message, by happenstance, were routed through the UK, the French operative could be tried and convicted under the law of the UK. There would, of course, still be the sticky situation of obtaining jurisdiction over the Frenchman. If he were operating under the direction of the French government, France would be unlikely to turn him over. On the other hand, the Frenchman may be well advised to vacation somewhere other than England for fear that authorities there would seize him upon his entering the country and try him.

Principle of Chivalry. The third basic principle of the law of armed conflict is the principle of chivalry. Its premise is that the waging of war should be done "in accord with well-recognized formalities and courtesies."[34] This principle recognizes that deception is often key to military victory and does not outlaw its use, but it does circumscribe how and when it may be used

within the broad constructs of *ruses* and *perfidy* (or treachery).

By international treaty, "[R]uses of war . . . are considered permissible."[35] Ruses consist of the use of trickery without reliance on any protected sign, symbol, or status. The use of misinformation to convince the Iraqis that the United States would attack from the shore was a proper use of a ruse. The ruse was designed to encourage the Iraqis to set up their troops to defend an attack from the shore, and thereby allow for more effective attacks against relatively unprepared forces away from the shore and an unsupported Iraqi rear flank.

Perfidy on the other hand is prohibited under the law of armed conflict. Thus, Protocol I to the Geneva Conventions states, "It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy." The protection that one is obliged to accord an enemy is largely identified by certain protected symbols that have been set out in a series of international agreements.

Various treaties have established protected status for symbols designating medical activities,[36] historic, artistic, scientific or cultural objects,[37] civil defense,[38] prisoner of war camps,[39] civilian internment camps,[40] and dangerous forces.[41] The UN emblem, the flags, uniforms and aircraft markings of neutrals and of the enemy and the white flag of surrender[42] also all denote a special status.[43] None of these symbols would seem likely to come into play in information warfare operations. The protected status recognized by these symbols, however, may. For instance, suppose Iraq sent a bogus E-mail message to low-level coalition force commanders in the Persian Gulf purporting to be from the commander of all coalition forces indicating that Iraq has surrendered and all hostilities are to cease immediately. If a commander acted on this message, believing it to be real and suffered heavy casualties from an Iraqi force he thought was surrendering but was actually attacking, would Iraq be guilty of violating the law of armed conflict? The question raised is whether such action constitutes a ruse or perfidy. Arguably, although Iraq did not directly claim to be surrendering, its act of spoofing the United States into so believing and taking advantage of the protected status of surrendering troops, may well place its actions into the category of perfidy and therefore constitute an LOAC violation.

Neutrals

The issue of neutrals may pose interesting legal issues under information warfare. Generally, nation-states desiring to maintain neutrality may not allow belligerents to cross their territory or to use their ports except to perform emergency repairs. How, then, does this general concept apply in the information era where communications channels criss-cross a nation's territory and may well be used by belligerents on either or both sides? The Convention on Neutrals[44] would seem to suggest that a neutral could condone the use of its communications cables without risking its neutrality:

> Art. 8. A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.[45]

However, if a neutral tried to prohibit the use of its communications channels to one of the belligerents, it would have to prohibit use of the same to the other belligerent(s) as well or place its neutral status in jeopardy:

> Art. 9. Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents.
> A neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.[46]

In point of fact, the common use of fiber-optic cables and packet-switched networks may well make it nearly impossible to deny the use of communications facilities to a belligerent without also denying those facilities to one's own popu-

lace. Significantly, the treaty does not address telecommunications satellites, though the same problems may well exist in selectively denying use to some users without jeopardizing all users.

Conclusion

General Fogleman was insightful for rec ognizing the importance of ascertaining the legal boundaries and implications of activities taking place under the catchphrase of information war - fare. Unfortunately, for the same reasons that many recognize this information age as a third wave or new era, many of the issues now being raised are without clear precedent. This paper has dealt only with the customary international law implications, and in this arena we see that most of the law to which legal scholars are looking for guidance was developed, in many cases, decades before informa - tion warfare concepts were envisioned. Nevertheless, certain basic principles can be carried forward—principles such as military necessity, proportionality, and chivalry. The specifics on how these general principles will be applied to certain specific information warfare scenarios will likely require gradual honing. As countries begin to agree on certain standards, these may well develop into a new customary interna tional law. More immedi - ate desires for regulatory guidance may prompt nations to seek consensus through the treaty-mak - ing process. Some prominent thinkers in this area have claimed that our first- and second-wave le - gal system is so hopelessly unable to deal with third-wave issues that it must be replaced promptly and ignored to the extent necessary in the interim. This seems an overreaction prone to anarchy. On the other hand, some claim that the issues raised by information warfare are really no different than those that have been raised throughout time and that thoughtful application of the existing law is all that is needed. This ex - treme also seems off the mark and betrays a na - iveté of dealing with complex issues in an entirely new realm. However, for now we have only the existing law and must apply it as makes best sense, working to fill the law's gaps as they are identified. The fast-moving world of the third wave will provide chal lenges in accom - plishing this, but the ease and speed with which information can be exchanged may also facilitate the task. □

Notes

1. Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (San Francisco: W. H. Freeman, 1976), as cited by Manfred Lachs, "Views from the Bench: Thoughts on Science, Technology and World Law," *American Journal of International Law* 86 (October 1992): 673. Lachs is a judge and former president of the International Court of Justice.

2. "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post,* 16 July1996.

3. "Onward Cyber Soldiers," *Time,* 21 August 1995, 44.

4. Ibid., 40.

5. "The Pentagon's New Nightmare."

6. John Arquilla and David Ronfeldt, of the Research and Development (RAND) Corporation, have defined information warfare as being the sum of netwar and cyberwar. *Netwar* they define as "societal-level conflict waged through Internetted modes of communication." *Cyberwar* they define as "conducting and preparing to conduct military operations according to information principles."

7. This was the working definition recognized by the School of Information Warfare and Strategy of the National Defense University as of 16 November 1993.

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

9. Ibid., 3.

10. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 13.

11. Richard Power, *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare.* (San Francisco: Computer Security Institute, 1995).

12. Ibid.

13. "The Pentagon's New Nightmare," C-3.

14. *Cornerstones of Information Warfare* , 3. This definition is similar to one proposed by the Office of the Assistant Secretary of Defense for C^3I.

15. The Law of Armed Conflict also applies to certain conflicts internal to a nation-state, but that is beyond the scope of this paper.

16. Lt Col William J. Fenrick, "The Rule of Proportionality and Protocol I in Conventional Warfare," *Military Law Review* 98 (1982): 91. Colonel Fenrick was a legal officer with the Canadian Forces.

17. Jean S. Pictet, *ed., Commentary, Geneva Convention Relative to the Protection of Civilian Persons in Time of War,* vol. 4 (Geneva: International Committee of the Red Cross, 1958), 20.

18. The legal ambiguities raised by cyberspace are not unique to discussions of information warfare. Computer crimes have raised some of the same issues. To what extent can Muslim countries enforce their criminal sanctions against the importation of pictures of scantily clad women when Internet sites around the world offer such pictures to anyone with a modem or other means of accessing the Internet? Or take the example of offering unauthorized gambling nationwide. One Internet site in the Turks and Caicos islands of the West Indies is already doing so, despite the objections of the US Department of Justice. So far the Justice Department has been unable to prevent the gambling site from continuing its operations.

19. The Air Force Judge Advocate School, *The Military*

Commander and the Law (Maxwell AFB, Ala.: Judge Advocate School, Center for Professional Development, September 1994), 580.

20. Section I, par. 14, *Instructions for the Government of the Armies of the United States*, prepared by Francis Lieber and promulgated by President Abraham Lincoln in 1863 as General Orders 100. Reprinted in *The Laws of Armed Conflict: A Collection of Conventions, Resolutions, and Other Documents*, ed. Dietrich Schindler and Jiri Toman [Rockville, Md.: Sijthoff and Noordhoff, 1981), 3–8..

21. Col Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, no.1 (Winter 1994): 37.

22. Ibid., 37–38.

23. *Cornerstones of Information Warfare*, 3, note 1.

24. Science Applications International Corporation, "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," research report for the chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C., 4 July 1995. The fact that a country's military uses civilian communications for a large portion of its message traffic increases the justification for claiming such a target is a military target.

25. *The Military Commander and the Law*, 580.

26. Field Manual (FM) 27-10, *The Law of Land Warfare* , 18 July 1956, Article 34.

27. Some may claim the convention did not "add" these weapons to the list of forbidden weapons, but reduced to writing that which, over time, had already come to be recognized by many countries around the world.

28. Protocol I to the Geneva Convention of 1981, Article 36. Indeed, a new "means or method" of warfare requires a similar determination under the article.

29. Executive Order 12333, "United States Intelligence Activities," 4 December 1981, *Codification of Presidential Proclamations and Executive Orders, January 20, 1961–January 20, 1985* (Washington, D.C.: Government Printing Office, 1986), 582–83.

30. Firewalls are computers that serve as protective front ends to a network. All traffic that seeks access to the network must pass through the firewall computer, which is designed to ferret out intruders. Root access is that access level that allows the user to execute the widest range of commands. Such access is normally only afforded to the system operator. Hackers who obtain such access can wreak havoc on the system.

31. Computer Misuse Act, 1990, section 1(1).

32. Ibid., section 4(2).

33. Ibid., section 5(2).

34. *The Military Commander and the Law* , 581.

35. The Hague Regulations of 1907, Article 24.

36. Red Cross, Red Crescent, Red Lion and Sun, or Red Star of David (Article 38, 1949 Geneva Convention I, and Article 18, 1977 Geneva Protocol I to the 1949 Geneva Conventions. The Red Lion and Sun is largely obsolete since on 4 September 1980 Iran indicated its intent to use the Red Crescent henceforth).

37. Red circle with triple red spheres in the circle on a white background (Roerich Pact of 1935) or royal blue square and triangle on a white shield (1954 Hague Convention, Article 14, and the Hague Regulations, Article 20) or rectangular panel divided diagonally into two triangular portions, the upper black and the lower white (1907 Hague Convention IX, Article 5).

38. Blue triangle on orange background (1977 Geneva Protocol I to the 1949 Geneva Conventions, Article 66).

39. "PW" or "PG" on a square flag (1977 Geneva Protocol I to the 1949 Geneva Conventions, Article 23).

40. "IC" on a square flag (1977 Geneva Protocol I to the 1949 Geneva Conventions, Article 83).

41. Three bright orange circles of equal size on the same axis (1977 Geneva Protocol I to the 1949 Geneva Conventions, Article 56[7]).

42. A white flag is recognized as a symbol of surrender under Article 32, 1907 Hague Regulations.

43. Air Force Pamphlet 110-34, *The Military Commander and the Law of Armed Conflict*, 25 July 1980.

44. Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907.

45. Ibid.

46. Ibid.