DISTRIBUTION A:
Approved for public release; distribution is unlimited.

IW Cyberlaw

The Legal Issues of Information Warfare

MAJ DAVID J. DICENSO, USAF, RETIRED

SHOULD INFORMATION-WARFARE techniques be viewed as weapons or as another instrument of foreign policy? This article briefly delves into the treaties and laws governing warfare from an information-war perspective. Do these treaties and criminal laws prohibit the bulk of the most technologically effective techniques from being used, particularly during peacetime?

By and large, many of the legal parameters of information warfare (IW) are, as yet, ambiguous. This uncertainty can only be resolved through open and frank discussion of just where information-warfare operations fit into foreign policy, international relations, and the international legal environment. The problem is that a nation or actor may well take advantage of the ambiguities that exist and force us to attempt to resolve these issues long before we are prepared to even address them. This article is a modest step to suggest a paradigm for analysis of these issues before we find ourselves backed into the proverbial corner and are forced to choose between no response and a vigilante-style response.

Do these treaties and criminal laws prohibit the bulk of the most technologically effective techniques from being used, particularly during peacetime?

What Is "Information Warfare"?

Although it seems clear at first blush, the term *information warfare* means different things to different people. There is little agreement on an accepted definition. *Information warfare*, *attack-mode* and *defensive-mode warfare*, *electronic warfare*, *cyberwarfare*, *cyberwar*, *soft war*, *hacker warfare*, and *low-intensity warfare* are just a few of the terms that are used in information-warfare circles to describe the same general concept.[1]

Sun Tzu thought of information warfare as including all elements necessary to win without fighting. He advised that you should "assess your opponents; cause them to lose spirit and direction so that even if the opposing army is intact it is useless."[2] This suggests that the scope of information warfare has, from the very beginning, been all-inclusive and embraces every aspect of information use that would permit war without battle. This seems to include the modern notions of human intelligence (HUMINT), electronic intelligence (ELINT), communications intelligence (COMINT), psychological operations (PSYOP), and every other method of gathering and affecting information that may be used to the advantage of one nation or to the detriment of another during a conflict.

Gen Ronald R. Fogleman, former Air Force chief of staff, has referred to the information explosion and the proliferation of interest in information operations as the "fifth dimension of warfare."[3] He describes the land, sea, air, and space as the first four dimensions.[4] He characterized information warfare 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."[5]

Alvin and Heidi Toffler were among the first to meaningfully address the modern information explosion and its impact upon society. They speak of our next conflict as being an "anti-war." They characterize the latest information revolution as the "information age" much like the agricultural age and the industrial age.[6] They recognize that knowledge is the "central resource of destructivity just as it is the central resource for productivity.[7] "Knowledge is what the anti-wars of tomorrow will be about."[8] The Tofflers' opinions suggest that the breadth of information warfare is all-encompassing, including all forms of knowledge.

The National Defense University (NDU) defines information warfare as the "aggressive use of information means to achieve national objectives . . . the sequence of actions undertaken by all sides of a conflict to destroy, degrade, and exploit the information systems of their adversaries," and it also includes actions intended to protect systems against hostile actions.[9] The Information Warfare Center at Kelly AFB, Texas, casts a wide net in its definition of information warfare. Its view is that information warfare is "broadly considered to be the use of computer, satellite, telephone and other systems to damage, destroy, degrade, exploit and interfere with command and control (and other) systems of an adversary or potential adversary and the use of such techniques to deny an enemy or a potential enemy the ability to do damage, destroy, degrade, exploit or interfere with similar systems owned and used by the US."[10]

This view, and an industrial or commercial notion of "information assurance" or defensive methods to protect information assets, are probably the best conceptualizations we can adopt to describe the specific military information environment relevant to the issues that follow. It is the one that is adopted for the remainder of this article. However, IW is generally much broader in scope than those technology-oriented aspects relevant here.

"What is an act of war in cyberspace? Is a personal computer or Unix-based system a 'weapon'? Is hacking through the communications systems of a hostile nation an 'attack'?"

What Can the United States Legitimately Do?

The resolution of this issue requires an exhaustive search for guidance. Space law, telecommunications law, international law, criminal law, and the Law of Armed Conflict (LOAC) are all applicable to some degree. One must examine these sources as a whole body of law in order to derive a valid and effective framework for resolving this issue.

Laws bind the nation that created the law, but they generally do not bind other nations. Laws can be enforced in the court system of the country that has jurisdiction over the offense. Treaties are agreements between nations regarding issues that will have some type of mutual impact upon them. Treaties are essentially contracts between nations and bind only signatory nations. Customary laws are the unwritten rules by which nations interact. Treaties and customary laws are enforced in a variety of ways through the International Court of Justice (ICJ), domestic law, arbitration, or the convoluted political process, for example.

Does the UN Charter Apply to Information Warfare?

The initial treaty that one thinks of when considering international issues and conflict is the UN Charter. Unfortunately, it was drafted in terms of armed aggression, not information wars. The UN Charter provides for the relationships of nations in joint, multinational activities of diverse types, not just in times of war.[11] Article 2(4) of the charter indicates that "all members shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any state." Two ICJ cases, the Corfu Channel case and the Nicaragua case,[12] suggest that

Article 2(4) of the UN Charter is violated any time a country resorts to aggression in an attempt to force another country to undertake a particular action. This is a codification of international relations reflecting a concept transcending treaties—the manifestation of the fundamental notion of sovereignty. This age-old concept remains as strong as ever in guiding the course of international relations as well as both domestic and foreign policy. The concept is a fundamental starting point for any analysis of international law issues.

Does Space Law Apply to Cyberspace?

This question is easy to answer in traditional lawyer's terms: It depends. It is dangerous to simply equate outer space with cyberspace. Although some people may conceptualize both as a free space without territorial boundaries, that approach may run afoul of various laws, treaties, and customs. Regardless of one's interpretation of cyberspace, the basic relationship is clear: A person at one location is using a computer to negatively impact another individual or organization at another location. Telecommunications has long been viewed as a medium, not a location. This traditional analysis views the use of computers for "information warfare" as simply the utilization of a more advanced communications system.[13]

The space-related treaties (space law) appropriate to consider in this context are the Outer Space Treaty, the Moon Treaty, and the Liability Convention. The United States has agreed to each of these treaties. Each shares a common underlying principle, although not always clearly articulated: The use of space will be limited to peaceful purposes.[14] This was recognized by the United States in the amended National Air and Space Act (NASA) of 1958[15] and 42 US Code (USC) 2451, wherein "the Congress hereby declares that it is the policy of the United States that activities in space should be devoted to peaceful purposes for the benefit of mankind."[16] This clearly diminishes the potential for unrestrained use of space for hostile purposes.

The Outer Space Treaty indicates that parties agree "not to place in orbit around the earth any *objects carrying nuclear weapons or any other kinds of weapons of mass destruction*" (emphasis added).[17] The italicized text of this passage indicates the ambiguity of the treaty.

What is a "weapon of mass destruction"? This generally refers to nuclear, biological, or chemical weapons. When this treaty was penned in 1967, the escalating computer power and cyberwarfare capabilities were probably not foreseen by the drafters. Some have interpreted this treaty to mean that it does not include communications equipment that could transfer data between two or more terrestrial points and is thus excluded by a "strict" reading of the treaty.[18] This interpretation, while legally accurate, necessarily avoids the practical consideration of the devastation that could be caused, by corruption or manipulation of information, upon members of the victim nation. How can one claim that shutting down utility grids, transportation systems, and banking systems is not "mass destruction"? Under the conventional use of the phrase, as discussed above, it simply does not qualify from a legal standpoint. Should it? It seems that if the satellite carries communications equipment that is an integral part of a larger system that actually causes or precipitates "mass destruction" upon the enemy, then the satellite is indeed carrying a vital component of the weapon system as a whole.

This begs for a definition of a "weapon system." In this regard, the US Marine Corps seems to be forward-thinking. They look not to the physical aspect of an item, but its intended use.[19] Thus, if satellite communications equipment were intended to be used for purposes of offensive or "attack-mode" warfare, it would require the same review as any other weapon system prior to its acquisition. For all practical purposes, this approach seems to unilaterally place communications equipment meant for IW clearly

within the treaty definition. This is not, however, a settled issue.

What does the Outer Space Treaty mean when it prohibits satellites that "carry" the weapon? Some would argue that satellites would not actually be weapons, since they simply transfer information. As mere relays for the information warfare "weapon," the communications relay would not, in and of itself, be a weapon subject to the treaty.[20] Again, this technical view does not consider the essential relay system as part of the whole weapon. A personal computer in isolation is not capable of an attack upon another nation's infrastructure; but when combined with telecommunications satellites capable of expanding the computer's influence to a nation in a distant area of the globe, has not the communications equipment aboard the satellite become part of the information "weapon"? This may be merely a semantic or philosophical argument, but it illustrates the ambiguity of the treaty.

The Outer Space Treaty isn't the only player on the field. The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the Moon Treaty) was created in 1979. It clearly prohibits the use of the moon as a military asset. Development and exploration of the moon must be conducted in a peaceful manner. The treaty attempts to assure that the use and exploration of the moon will not become an area that creates international discord. Moon-based communications equipment for information warfare purposes would seem to be simply prohibited. However, the United States has never ratified or signed this treaty. Although the United States is not bound as a signatory nation, these provisions should be considered before any such moon-based system is contemplated, if for no other reason than for political harmony and consistency in our foreign policy.

At first blush, the Convention on International Liability for Damage Caused by Space Objects (October 1973) appears to relate to cyberspace. This treaty, commonly referred to as the "Liability Treaty," requires a launching state to pay for any damages caused by one of its space objects if the object causes damage to the surface of the earth or to an aircraft in flight.[21] It also discusses space objects "launched" by a state, implying the intent to apply it to satellites, rockets, and other tangible space vehicles.[22] The treaty is vague enough that a "victim" state may claim that terrestrial information damage is fairly embraced by the language of the treaty itself if they are attacked or threatened. Since the concepts and capabilities involved in IW are such recent developments, an argument to impose liability under this decades-old treaty may be extremely weak.

Although these treaties exist and may have some impact upon information warfare, they provide little, if any, meaningful guidance. Recognition of these space-law considerations is vital, however, as they must be considered much as an infantryman would consider the location of mines while crossing a field; they are not necessarily roadblocks to our progress but have the potential to cause explosive and disastrous international legal problems if we run afoul of their provisions. Outer space and cyberspace may seem conceptually similar, but the legal mechanisms that we rely upon to resolve legal issues in outer space were created to resolve issues that simply do not exist in cyberspace. Space law was created to resolve issues that revolve around spacecraft or the use of celestial bodies. Simply put, space law will not help us resolve any of the issues we currently face in negotiating the legal landscape of cyberspace.

Does Telecommunications Law Apply?

The treaties known as International Telecommunications Satellite Organization Agreement (INTELSAT) and the Convention on the International Maritime Satellite Organization (INMARSAT) comprise the body of international telecommunications law that currently exists and is applicable to information warfare.

The INTELSAT (1973) broadly defines "telecommunications."[23] The treaty's intent is to ensure that a satellite will only be used for peaceful purposes. This broad prohibition includes virtually every aspect of information warfare data traffic. Fortunately, it also specifically articulates a position on satellite systems that have a military purpose. "This agreement shall not apply to the establishment, acquisition, or utilization of space segment facilities separate from the INTELSAT space segment facilities solely for national security purposes."[24]

Despite the impression that one might garner from the popular media, there actually is a substantial body of statutory law that applies directly to computer crime and hackers.

The International Telecommunications Convention of Malaga-Torremolinos (25 October 1973), Article 35, states that "all stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members." Thus, the treaty seems to prohibit the use of a satellite station to disrupt or somehow interfere with the communications of other states. Paradoxically, the same treaty states, in Article 38, that "Members retain their entire freedom with regard to military radio stations of their army, naval, and air forces." Thus, the treaty recognizes that there may, indeed, be a military use of a satellite system that would not otherwise comply with the earlier provisions of Article 35. However, since 95 percent of our military administrative traffic passes through civilian communications systems,[25] one must ask if this is a "military" system for purposes of Article 38 or if it is a "civilian" system that is protected under Article 35.

Why is the "civilian versus military" distinction relevant? When INTELSAT is read in conjunction with the International Telecommunications Convention of Malaga-Torremolinos, it is clear that the military may not use civilian telecommunications satellites to assert military power, but may use a "military" satellite system for such purposes. Military telecommunications satellites, expressly excepted from the International Telecommunications Treaty of Malaga-Torremolinos, may be able to disrupt or interfere with the communications systems of other nations in the interest of national security, with the limits discussed earlier. The character of the communications satellites is thus critically important.

The INMARSAT (1976), Article 3(1), limits the use of the INMARSAT space segment to the improvement and facilitation of maritime communications. The treaty restricts the use of satellites owned or leased by INMARSAT to "peaceful purposes" only. Presumably this would prohibit the use of INMARSAT space segments for military purposes.[26] The intent of the INMARSAT is to prohibit the use of the satellite systems for military purposes other than navigation and routine communications similar to those in which a civilian maritime vessel would normally engage.[27] Generally, the quintessential interest in telecommunications seems to be the preservation of the tradition of noninterference.[28]

How Does Criminal Law Apply?

With the World Wide Web expanding at its current rate, the opportunities for those with ill intent abound. Most systems on our Internet are privately owned and are shockingly vulnerable to a cyberattack by a technically oriented person with criminal intent. Criminal law is an important and relevant area to consider when evaluating precisely what we can legitimately do. The law is specific and incorporates many fundamental constitutional considerations such as the user's right to privacy and the protection of the individual from unreasonable searches and seizures.

"Any analysis regarding information defenses or back hacking must be viewed from a criminal law perspective—at least until the source of the intrusion can be identified. . . . Once we have determined the identity of the unauthorized intruder or the origin of the intrusion, we can better determine who must respond, and how."

Despite the impression that one might garner from the popular media, there actually is a substantial body of statutory law that applies directly to computer crime and hackers.[29] Computer crimes are federal offenses.[30] Government computers and computers that are merely used by or for the government are protected,[31] as are computers used "in interstate commerce or communications."[32] Obviously, any computer that accesses the Internet will likely fall squarely within this statute. One who knowingly causes the "transmission of a program, information, *code*, *or command* and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" in interstate commerce has committed a federal crime as well (emphasis added).[33]

The Access Device Fraud Act protects computer passwords, the use of access devices is prohibited, and use of access device-making equipment is similarly outlawed.[34] Title 18 also provides some password protection to stolen and fraudulently obtained passwords which could then be used to access computers by unauthorized individuals to wrongfully obtain things of value.[35]

Unauthorized interception (or intentional disclosure of the contents of unauthorized interception) of wire, oral, or electronic communications is prohibited by federal law.[36] There are several exceptions, the most notable of which is that so long as one of the parties in the conversation has consented, the interception is permitted.[37] The statutory framework also provides for civil liability for

unauthorized interception of communications.[38]

Unauthorized access to stored communications is also prohibited, and creates civil liability on the part of the one who unlawfully obtained such access.[39] Federal law also proscribes intentional unauthorized access to "a facility through which an electronic communications service is provided" if the person achieving such access "obtains, alters, or prevents authorized access" to communications while the data is in storage.[40]

Federal statutes exist to protect federal records, property, or public money.[41] Thus, bank and credit records are protected,[42] as are electronic fund transfers involving interstate commerce or foreign commerce.[43] Mail fraud is proscribed.[44] So is using a remote terminal or computer to further a fraud where messages cross state lines.[45]

Since making false or fraudulent statements to a government department or agency is prohibited,[46] a hacker who intentionally and falsely represents himself electronically to be an authorized user in a government computer system may violate federal law.

Of particular interest to the Internet community is the Privacy Protection Act of 1980.[47] This statute provides protection to electronic bulletin board systems (BBS) operators. BBSs may still be searched, however, if the government meets a specified criteria and obtains the proper authorization.[48]

E-mail interception is governed by existing telecommunications law. Intercepting the communications and accessing the communications are possible if they meet the criteria of the law's exceptions, with proper search authority, or with a court order.[49]

Why are all of these criminal laws important to help us determine what the military can legitimately *do?* Until the identity of the hacker is known, we must obey the criminal laws. These laws apply to us as well as to the hacker. Once the hacker is identified, however, different approaches may be appropriate (more on this later).

Search and seizure laws vary radically from country to country, and the biggest problem law enforcement authorities face is the chaos that seems to arise when the hacker is located in, or electronically travels through, a foreign country. For example, while we recognize an exception to our Fourth Amendment warrant requirement if there is exigency or "hot pursuit" to apprehend a criminal,[50] not all governments would recognize, or even care, about a US constitutional amendment exception when the United States seeks to intrude into their systems without preexisting authority. Imagine a hypothetical hacker, located in New York, who hacked through a commercial computer system into a computer in France, then on to a government computer in Taiwan, then through a Chinese military installation, back to South Korea, on to an installation in North Korea, then to the Japanese Defense Force computer system on Okinawa, and finally, back to the United States, where the hacker unlawfully enters a NASA computer. Consider the international uproar if North Korea and China perceived the United States government's pursuit of the hacker to be an intrusion upon their military information systems. Suppose they view the initial hacker as a user and the person "back hacking" through their system as the hacker. The political ramifications are magnified considerably if they then determine that the hacker turns out to be a US government or law enforcement agent! This is an area where politics is clearly a paramount concern and may be at odds with obvious national security concerns.

In the cases of Rome Labs and the Argentine Intrusion, the hackers electronically traveled through foreign nations before reaching their intended targets. In each case, the primary problem in rapidly identifying the intruder was obtaining the cooperation of the international police agencies and governments involved.[51]

The Council of Europe recently convened to address this issue. It was clear that the various nations need to work together toward standardized uniform criminal proce-

dures. After evaluation of the problems involved, the council recommended that "the power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established.[52]

Investigation of federal computer crimes in the United States is generally within the purview of the Federal Bureau of Investigation (FBI). If a foreign source of an electronic intrusion is identified, the Central Intelligence Agency (CIA) would become involved. The Secret Service is the office of primary responsibility when the intrusion has financial implications. While the Defense Information Systems Agency (DISA) handles security breaches in military computer systems, the Air Force's Office of Special Investigations (AFOSI) is deemed a leader in developing investigation strategies and is generally given a great deal of freedom in investigating incidents involving Air Force computers.

It seems that there will be some international effort to resolve the incompatibility of criminal law at some point in the near future. Until such time, the best way for law enforcement to track hackers through diverse jurisdictions is through close coordination with investigators in the host countries and in strict compliance with their laws. This approach is not particularly rapid or efficient, but it respects the all-important concept of national sovereignty and causes no adverse international political ramifications.

The Law of Armed Conflict

Much of our international law is merely a recognition of the "customary laws" of nations. Some of these have been codified and have become treaties, while yet others remain as mere manifestations of accepted traditional international practice.[53] The rules governing the conduct of nations and combatants during hostilities are known collectively as the Law of Armed Conflict. The LOAC is simply that part of international law that represents an attempt to regulate conduct during armed hostilities in a manner that is practical (so that it will not impede the waging of war) but to nonetheless minimize its savagery. Whether war is waged on the muddy fields of Verdun by shell-shocked infantry troops or a high-tech cyberspace battlefield, the rules and general principles of the LOAC remain applicable.

The primary conventions that codified the concepts of war-fighting principles are found in the various Hague and Geneva Conventions.[54] Basically, the Hague Conventions can be thought of as "offensive" in nature, while the Geneva Conventions deal with the treatment of the sick, wounded, and prisoners of war; these may be collectively considered mere "defensive" provisions. These conventions are now the nucleus of the LOAC.[55]

Their primary objective is to ensure that hostilities are directed to defeat enemy forces, not to injure innocent civilians or other noncombatants. The LOAC is an attempt to protect everyone, combatant or noncombatant, from unnecessary suffering, savagery, and brutality that accompanies armed conflict. It is a method to facilitate the restoration of peace following the conclusion of armed hostilities.

Typically, the main principles of the LOAC are military necessity, humanity, proportionality, and chivalry. These fundamental principles are used as a guide in interpreting the LOAC and in reaching an appropriate conclusion when particular circumstances do not specifically fit within the parameters of existing rules.[56]

The LOAC provides combatants with certain rights and privileges if wounded or captured in wartime, and it proscribes certain offensive activities. The Prisoner of War Convention identifies the "protected persons" under the LOAC.[57] Generally, civilians accompanying an armed force do not engage in acts of war—media representatives, contractors, civilian services personnel, and

so forth—are all deemed "Auxiliary Services" and are entitled to prisoner-of-war (POW) status if captured. If one of these individuals were to engage in a hostile act, that individual would be deemed an "Unlawful Combatant" and could be punished under the laws of the captor.[58] Spies do not receive any special treatment under the LOAC and are punished under the laws of the captor nation.[59]

The conventions and traditions seem clear and easy to understand, but when applied to information warfare, they become difficult to administer. To date, the rules and laws have been concerned with sovereign borders and physical invasion of those borders by armed belligerents. In cyberspace there are no borders. The landscape is an unbroken terrain of network connections between military and civilian computer systems that interact rapidly without regard to the artificial lines on a map that designate international borders. The threat comes from computer technicians who may be able to disable banking systems, electrical grids, airline traffic control systems, and communications equipment. At what point are these actions serious enough for a victim nation to respond with force? What is an act of war in cyberspace? Is a personal computer or Unix-based system a "weapon"? Is hacking through the communications systems of a hostile nation an "attack"?

Air Force Policy Directive (AFPD) 51-4, *Compliance with the Law of Armed Conflict*, par. 2, requires Air Force personnel to comply with the rules "during armed conflict." The AFPD defines *armed conflict*[60] as a situation where at least one state has begun to use armed force. However, there is no guidance on what legally constitutes "armed force." Logically, to use armed force, one must utilize an arm or weapon of some type.

Air Force Instruction (AFI) 51-402, *Weapons Review,* May 1994, suggests computer systems would probably not be considered weapons. "Weapons are devices designed to kill, injure, or disable people, or to damage or destroy property. Weapons do not include . . . electronic warfare devices."[61] Even though the computer itself would not be thus deemed a "weapon," it could, indeed, do substantial damage to an enemy's war-fighting capability.[62]

None of these issues have yet been resolved. It is not surprising that the LOAC is not up to date in regard to IW. During World War I, no provisions existed for aerial warfare; principles had to be developed from the existing rules that governed ground warfare and naval bombardment. Only after seeing the results of applying land warfare rules to bombing did the thought arise to develop a code specifically designed to address air warfare.[63] The LOAC is dynamic and evolves along with new technology and the war-fighting capabilities of various nations.

Even though damage may be done to a nation's capabilities, there is no authority to suggest that a computer is a weapon or that an information operation act is an "act of war." Of course, if a hostile nation defines the act of war based on damage caused or damage potential instead of the character of the item used to commit the act, the analysis would be quite different. Although this view may not favor the nation with the technological edge, it is the most logical conclusion. If death and destruction resulted from the IW operation, an armed response by the victim nation would probably be warranted. If we were to cause a power grid shutdown in a foreign country, it could foreseeably lead to civilian riots; hospitals could have unforeseen casualties from failing life-support or otherwise relying upon the power grid for public health purposes; mass transit in major cities could be disrupted bringing a concomitant economic disaster when workers cannot get to their place of employment; and the financial system could be disabled. The potential adverse repercussions could be remarkably dramatic. It would be difficult, indeed, to convince the victim nation that this intentional vulnerability exploitation by an unfriendly nation was not an act of war. If even minor disruptions can cause violent outbursts and disarray,[64] imagine the repercussions of intentional and strategic manipulation of a country's infrastructure systems.

Military retaliation by the victim country should be an expected consequence of such an electronic attack.

Defensive Application of the LOAC to Information Warfare

Defensively, there does not seem to be any issue of great legal significance. A nation may protect its information or systems in any way it chooses so long as it does not negatively impact another nation or another nation's communications systems. Issues such as encryption and various other aspects of cryptology are currently raising a great deal of interest, but at this point, the issues raised seem to be those of policy and strategy, not of law. Offensively, the character of the problem is quite different.

Offensive Application of the LOAC to Information Warfare

What are some of the offensive possibilities? Could we attach a "logic bomb" to DOD information, so that a hacker who obtains the information also obtains the "bomb" that destroys his computer system? Could we engage in "active defense" where we intentionally send destructive code to his machine upon realization and confirmation of the unauthorized penetration of the DOD system? Could we send him a "worm" to infect and/or disable his system?

We can do none of these things. Without identifying the infiltrator, we cannot even determine whether it is a national security issue. The new amendment to the Computer Fraud and Abuse Act of 18 USC 1030 (a)(5) prohibits the intentional destruction of data in computers without regard to whether the person "attacked" was initially authorized access or not. Such activity is a federal felony. Additionally, if the attacker wove his way through several different systems before "attacking" the DOD computer, and in response, we sent a destructive code to him, there is a possibility that every system along the way would also be damaged or corrupted. This could be disastrous if he were using a government computer or accessing the information through yet another government computer. But what if the hacker were a teenager using a civilian parent's computer where his parent ran a business out of the home, such as a dentist, accountant, lawyer, or other professional? Taking down the computer system with client records stored therein could have unintended consequences, potentially very costly ones. How could fast responses ensure that collateral damage is minimized or at least considered? There seems to be no effective way to undertake "active" defenses that would be acceptable, either legally, conceptually, or practically. The preferable approach may be to use additional (self-altering) passwords and advanced encryption or even several layers of encryption if necessary.[65]

> There is seldom a clear point at which we can identify the mythical act of war.

Discussion of an act of war seems to be in vogue right now in information warfare circles. Even casual rumination on this point would lead to the conclusion that it is "a singularly imprecise and unhelpful concept" that became passé a half-century ago.[66] Conflict is a process of escalation. If a country engages in an unfriendly conduct of some type, then the adversely affected nation would likely respond "offensively." This is not a progression of distinct stages but rather an unbroken continuum where unfriendly acts become increasingly hostile. There is seldom a clear point at which we can identify the mythical act of war. International concerns from both a political and legal perspective must always be considered any time a nation seeks to engage in unfriendly activity where another nation may suffer. Unfriendly acts have been used for hundreds of years to encourage a nation to comply with a particular demand of another

country. A naval blockade is an age-old example of an "unfriendly act" intended to direct or control another nation's actions. Economic embargoes and blockades are also unfriendly acts with concomitant adverse international impact. Both have been historically viewed as unfriendly acts, but not necessarily acts of war.

I submit that even in peacetime, however, the principles behind the LOAC remain applicable at all times.

Is there an electronic parallel between an economic embargo and an information embargo? Information isolation is an analogous counterpart to the naval blockade of yesteryear. These activities occur outside of the nation's borders, whether the blockade is a physical one or an electronic one. A blockade is not an act of infiltration, as an attack would be. An electronic blockade would create a similar isolation, only it would apply to the nation's electronic networks. In such a scenario, an electronic embargo or blockade would (and should) be subject to precisely the same political and policy considerations as its eighteenth century counterparts.[67] The low-level unfriendly activity of these types is nothing new; only the medium has changed in size, scope, and complexity from physical coordinates to cyberspace.

Offensive information warfare using computer technology should be viewed as an escalation of hostilities instead of an act of war. This commonsense approach would better reflect the reality of politics in international relations. Escalation of hostilities may reach the point where actual physical damage is caused by a belligerent nation's armed military force; the rules of the LOAC are then clearly and unequivocally applicable. An example of this is the 1986 bombing of a disco in Germany by state-sponsored terrorists from Libya. Our response was to bomb several military sites in Libya including the Tripoli Airport, the Aziziya barracks, a naval base and airfield, and the port of Benghazi.[68] This response by the United States was well within the parameters of acceptable behavior of a nation under the LOAC.

If the offensive use of computers to disrupt, corrupt, interfere with, or deny enemy computer and information system utilization does not equate to an armed conflict, then the LOAC would (arguably) not apply to the offensive-mode computer intervention in another nation's systems.[69] This, it seems, is a troublesome interpretation of the applicability of the LOAC to cyberwarfare. It would leave the door wide open for offensive use of computers with no checks or balances upon such use. It suggests that the principles, discussed above, would not apply in the absence of armed conflict.

It would seem that many electronic activities have clear parallels to traditional "physical" actions that a nation may take. If one were simply to equate the electronic action to a physical act according to the damage done, the analysis is much less problematic. In these cases, traditional LOAC analysis applies.[70] I submit that even in peacetime, however, the principles behind the LOAC remain applicable at all times.

The Law of Armed Conflict obviously applies to "armed" conflict. Traditionally, this has implied a physical invasion or confrontation. It seems readily apparent from a conceptual viewpoint that computer warfare should be governed by the traditional laws of armed conflict, but the terminology used in our conventions does not clearly apply. To casually dismiss the applicability of the LOAC simply because the LOAC does not apply under a strict, literal reading of the conventions would be a simplistic approach by a nation that would be inclined to exploit this loophole. The danger is that such a loose (and arguably inappropriate) reading of the laws is that it works both ways. The nation that seeks to exploit a vulnerability of another nation then later claims that the LOAC does not apply should beware that it may be the victim of a cyberattack by a similarly disposed nation. Under such circumstances, the hapless victim of the attack would likely change its definition rapidly and claim a contrary interpretation of the LOAC.

It is critical that these issues be resolved as soon as possible to prohibit or inhibit the gamesmanship that these ambiguities invite.

Does a nation forfeit its neutrality if communications from a belligerent nation travels through communications relays physically located inside the neutral's borders? Information warfare operations are as likely to travel through neutral countries as any others before reaching the belligerent target. Computer telecommunications travel through cyberspace in exactly the same way as routine telephone traffic. A single telephone conversation may travel through several different links. Part of the conversation may occur through a set of links that automatically shift to another route without disrupting the connection while remaining transparent to the user.[71] There is no sure way to know exactly what route an information attack would travel over the international telecommunications systems in getting to the target belligerent. However, unintentional intrusions of a belligerent into a neutral country's communications systems is not deemed an LOAC violation, nor does the neutral nation forfeit its neutrality.[72] Of course, if a neutral nation were to restrict one belligerent nation from using its telephone relay systems while allowing such use by another belligerent nation, then a different analysis would apply. If the same telecommunications systems are open to all, and the use by belligerents is not intentional, then there is no threat to the neutral nation's claim of neutrality.

Jurisdiction and Information Warfare Investigations

During the Vietnam conflict, the US Army was called upon to respond to a variety of violent outbreaks of protesters. The Army worked in conjunction with local law enforcement and quickly found that the intelligence available regarding potential adversaries was inadequate. The US Army Intelligence Command (USAINTC) developed an "elaborate, nationwide system with the potential to monitor any and all political expression. No person was too insignificant to monitor; no activity or incident too irrelevant to record."[73]

Even though the DOD prohibited the collection of civilian surveillance in the 1970s and mandated the destruction of the records that had been compiled already,[74] both the House and Senate formed select committees to monitor the military surveillance data collection and act as an oversight committee.[75] The Intelligence Oversight Committee acts as a check upon the military's potentially invasive investigation and database building capabilities.

Covert IW activity[76] is governed by federal law.[77] The president of the United States must submit a finding to Congress, in writing, that details exactly why the foreign policy activities of the United States require the covert action and explaining why the action is important for assurance of national security.[78]

Even the CIA must obtain a Presidential Finding before conducting peacetime covert information-gathering operations.[79] DOD is tasked to respond to CIA needs by the director of the CIA; DOD is the only primary agency for signal intelligence activities through the National Security Agency (NSA).[80] The Treasury Department is responsible for collecting information related to financial concerns, monetary information, and foreign economic information. The Treasury Department is authorized only to collect "overt" information.[81] Overt information collection is considered to be the gathering of data, where the target of the data collection is aware that they are giving information to the government agency which is engaged in the collection activity.[82] The State Department conducts information relevant to US foreign policy. Like the Treasury Department, the State Department is normally limited to collection of only overt information.[83]

All executive agencies are generally prohibited from participating in secret operations unless they obtain approval from the agency and the attorney general. Even then, the activity can only be undertaken as part of

a lawful FBI investigation or when the target of the surveillance is composed primarily of people with foreign allegiance and the investigators must reasonably believe that the target organization or people are acting on behalf of a foreign power.[84]

Collection of foreign intelligence information (data about capabilities, intentions and activities of foreign countries, organizations, and persons)[85] is permissible in the United States, and it must be gathered by the FBI or an intelligence component (with some prohibitions) and may not be collected if the purpose is to acquire information about an individual's domestic activity. Collection of intelligence data is allowed in international terrorist or international drug investigations, if needed, to protect a person or an organization.[86] Collection of information to protect US (or foreign) intelligence sources, or methods of collecting such information, is also permissible.[87]

The FBI is permitted to collect information in the United States if the efforts are to protect intelligence sources or methodology from unauthorized disclosure.[88] An intelligence component may only collect information regarding employees or contractors.[89] It may also collect information on past or present employee applicants. If the intelligence component is within the charter of the government agency, it may collect information about people that it reasonably believes to be potential sources or contacts. Such surveillance is deemed necessary to determine their credibility or suitability for utilization as contacts.[90] Overhead reconnaissance not specifically directed at US persons is also allowed, as is information about security investigations of personnel or communications security.[91] Information incidentally obtained that indicated involvement in a crime is permitted as well.[92] Lastly, information may be obtained by an authorized component or unit if it is "necessary for administrative purposes."[93] Although this sounds like a euphemism for a carte blanche authorization for the DOD, it would be unlikely for the National Security Authority (the president acting through the secretary of defense) to approve such an operation without a valid, necessary administrative reason.[94]

The DOD is not exempt from normal "civilian" rules that govern the conduct of computer operations. This is to say that there is no exemption from the US Constitution or various federal, state, or foreign criminal laws. The restrictions upon intelligence-gathering operations must satisfy the restrictions placed upon the activity by the rules of criminal law, foreign criminal laws, and international treaties. For information-warfare purposes, this restriction is by far the most onerous, as outlined in the criminal law section discussed earlier in this article.

Conclusion

My paradigm for analysis of these issues incorporates a criminal law "default." That is to say, any analysis regarding information defenses or back hacking must be viewed from a criminal law perspective—at least until the source of the intrusion can be identified. We must not act in any way that would damage the unauthorized intruder's computer or any intermediate systems, as we would not yet be able to ascertain the risks of taking affirmative, aggressive action against the intrusion.[95] Once we have determined the identity of the unauthorized intruder or the origin of the intrusion, we can better determine who must respond and how. Exactly how we proceed from that point depends upon the location of the hacker and an assessment of the potential collateral damage.

If the intrusion is by a US citizen or military hacker, then the investigation and recourse are undertaken by the appropriate government agency such as the FBI, CIA, or Secret Service. If the intruder is not a citizen, but constitutes a foreign power, then the FBI or CIA with DOD support would be the likely agencies to resolve the issue. All applicable international laws, treaties, and criminal laws would clearly apply.

During wartime, however, DOD is given wide latitude to undertake intelligence-gathering activities. During such times of conflict, the paramount concern would be national security. Many of the international customs and

treaties are simply disregarded during time of war, subject to some limitations (such as continued adherence to the Law of Armed Conflict). If covert operations in the interest of national security are planned, then the traditional criminal rules would not strictly apply, as prosecution of offenders would probably not be contemplated. At that point, we would be more interested in ensuring our national security instead of future potential prosecution of criminal offenders. Of course, such disregard of international agreements will only happen when directed by the very highest levels of our government, and only after the ramifications and repercussions of such activity is thoroughly examined. This rapidly evolves into an issue that emphasizes the political dimension and relies upon motivations rooted in domestic and foreign policy; it is not necessarily guided or constrained by the law.

Although this analysis framework seems vague, the issue can be resolved by always resorting to a criminal-law default. Once the system intruder's identity is known, we will be better able to assess the relative merits of our response alternatives. If the intrusion occurs in time of war, then the rules by which we play are slightly altered in the best interests of national security. If the issue is one of covert operations, then entirely different rules apply, as outlined above.

Information warfare techniques are best viewed as another instrument of foreign policy from an LOAC perspective. The problematic aspect of this conclusion is that the above-mentioned treaties and criminal laws would likely prohibit the bulk of the most technologically effective techniques from being used, particularly during peacetime.

There are many aspects of "cyberlaw" that are, as yet, still unclear. These uncertainties must be resolved. If a nation takes advantage of the ambiguities that exist, the time to resolve the issues may be upon us before we are prepared to address them. Under such circumstances, it is unlikely that we would obtain the result that would be in our best interests. The United States should seize the initiative on these issues and provide guidance and leadership that would help ensure that the ambiguities are resolved properly and in the best interests of the United States.

It has been clearly demonstrated that we are not giving the issue of computer system vulnerability adequate attention. From the neglected systems themselves to the neglected system administrators, we seem to be passively enabling the hackers, crackers, and miscellaneous unauthorized intruders to accomplish their goals. We must enhance the security of our systems and provide those involved in the operation of the systems with the recognition and training that they deserve. We realize our systems are shockingly vulnerable and must act much more quickly than we seem to be doing to rectify this unfortunate situation.

Despite the problems that we have experienced, the United States (particularly the United States military) seems to be increasingly proactive in taking decisive action. As vulnerable as we appear to be, it seems that we are still on the cutting edge in addressing information warfare and global cyberspace issues. The Council of Europe has recommended that we standardize our criminal procedures to facilitate the tracking of international hackers, and we must seize the initiative to properly influence the drafting and implementation of effective international agreements as soon as practicable. Although other countries recognize the problems, it seems that we (the United States) remain as the leaders in the realm of cyberlaw and in recognizing its importance in the information age. The present and future cost of losing our position of leadership in this area may be beyond calculation. It is imperative that we remain on the cutting edge, both in ensuring the responsiveness of domestic law and international agreements to the emerging technologies encountered in the on-line world; we have a chance to shape the very substance of future cyberlaw. If we fail to do so, we must become content to live under global treaties and practices that may not be wholly to our liking. We cannot afford to lose this unique opportunity. ■

Notes

1. Donald E. Elam, "Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare" (master's thesis, Naval Postgraduate School, June 1996), 14.

2. Sun Tzu, *The Art of War*, trans. Thomas Cleary (Boston, Mass.: Shambhala Publications, distributed by Random House, 1988), 67.

3. Gen Ronald R. Fogleman, USAF chief of staff, "Information Operations: The Fifth Dimension of Warfare," remarks delivered to the Armed Forces Communications-Electronics Association, Washington, D.C., 25 April 1995, *Defense Issues* 10, no. 47 (1995): 1–3.

4. Ibid.

5. Department of the Air Force, *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force, 1995), 3–4.

6. Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century* (New York: Warner Books, 1993).

7. Ibid., 71.

8. Ibid., 203.

9. *Definitions for the Discipline of Information Warfare and Strategy* (Washington, D.C.: School of Information Warfare and Strategy, National Defense University, undated), 37.

10. Col Richard A. McDonald, "Intelligence Law," Department of the Air Force outline created for the Air Force Information Warfare Center, 1.

11. Article 51 of the UN Charter states that "nothing in the present Charter should impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security" (emphasis added).

12. *United Kingdom v. Albania* (1949), International Court of Justice (ICJ) 4; and *Nicaragua v. United States* (1986), ICJ 1.

13. See, for example, The Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Article 8, The Hague, 18 October 1907.

14. See, for example, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, *United States Treaties and Other International Agreements* (UST) (Washington, D.C.: US Government Printing Office, 1976), vol. 18, 2410 (18 UST 2410), and *United Nations Treaty Series* (UNTS) (New York: Secretariat of the United Nations, (1970), vol. 610, 205 (610 UNTS 205), hereinafter the Outer Space Treaty. See also the Agreement Between the United States of America and the Union of Soviet Socialist Republics Concerning Cooperation in the Exploration and Use of Outer Space for Peaceful Purposes, April 1987. Interestingly, the treaties promote peaceful purposes by the signatory nations but do not limit them to "only" peaceful purposes, thus leaving an ambiguity for a single nation to explore potential uses that are not peaceful. Note that the use of the word *should* as a term of art leaves the door open for exceptions. Had these provisions been intended to absolutely forbid the hostile use of space under all circumstances, the drafters surely would have used the words *shall* or *must*.

15. National Aeronautics and Space Act of 1958, as Amended, see Public Law 85-568, 85th Congress; H.R. 12575, 29 July 1958; 72 Stat. 426.

16. Note once again the use of the word *should* as opposed to the words *shall* or *must*.

17. Outer Space Treaty, Article IV.

18. Maj Richard W. Aldrich, "The International Legal Implications of Information Warfare" (unpublished study, US Air Force Academy, Institute for National Security Studies, Colorado Springs, Colo., April 1996), 20.

19. Lt Col Gary Sharp, USMC, Joint Chiefs of Staff Legal Counsel's Office, interview with author, 9 July 1996.

20. Aldrich, 20.

21. The Convention on International Liability for Damage Caused by Space Objects, October 1973, 24 UST 2389; and *Treaties and Other International Acts Series* (TIAS) No. 7762, Article II (Washington, D.C.: US State Department, 1973), hereinafter the Liability Treaty.

22. Ibid., Article IV.

23. The International Telecommunications Satellite Organization Agreement (INTELSAT), 20 August 1971, Article I(j), hereinafter INTELSAT.

24. Ibid., Article XIV(g). Note that the term *space segment* is defined in Article I(h). Space segment facilities include not only the telecommunications satellite itself but also the related command and control equipment necessary to control the satellite.

25. Col Philip Johnson, Headquarters USAF/JAI, "The International Legal Implications of Information Warfare," in Air Force Publication (AFP) 110-34, *Commander's Handbook on the Law of Armed Conflict: A Primer on Legal Issues in Information Warfare,* October 1995.

26. One may argue that the aggressive use of an INMARSAT satellite communications system to protect the security of a nation qualifies as a defensive or "peaceful purpose"; this specious argument may exist, but it seems transparently disingenuous at best.

27. The counter argument is that if military "routine" communications traffic were to be passed over the satellites in anticipation of war, then the treaty would apply and prohibit such communications. This argument is probably not convincing, however, because if the traffic passed is navigational, as opposed to tactical, in nature, then the communications could hardly be distinguished from civilian navigational telecommunications.

28. This sentiment of communications noninterference is echoed in the United Nations Convention on the Law of the Sea, Article 109, that prohibits broadcasting from the high seas to cause interference with coastal radio broadcasts.

29. For an in-depth discussion of criminal investigations and a more detailed application of federal statutes, see the "Legal Guide to Computer Crime," prepared by the Office of the Staff Judge Advocate, Air Force Office of Special Investigations, by Lt Col John T. Soma USAFR; Elizabeth A. Banker, Headquarters AFOSI/JA; and Alexander R. Smith, University of Denver College of Law (hereinafter the OSI Guide). See also the "Federal Guidelines for Searching and Seizing Computers," July 1994, by the US Department of Justice Criminal Division and Scott C. Charney and Martha Stansell-Gamm of the Computer Crime Unit (hereinafter the DOJ Guide). Both of these sources are excellent resources for thorough evaluation of the criminal investigation and prosecution process, and they were the sources from which I gleaned the bulk of criminal law citations for this project.

30. The Computer Fraud and Abuse Act of 1986 and the Computer Abuse Amendments Act of 1994 (18 USC 1030) both deal with crimes using computers.

31. 10 USC 1030 (a)(3).

32. 10 USC 1030(a)(5).

33. 18 USC 1030 (a)(5)(amended).

34. 18 USC 1029; and *United States v. Fernandez*, 1993, U.S. Dist. LEXIS 3590.

35. 18 USC 1030(6).

36. 18 USC 2511.

37. 18 USC 2511 (2)(d).
38. 18 USC 2520.
39. 18 USC 2707.
40. 18 USC 2701(a).
41. 118 USC 641; and 18 USC 2071.
42. 18 USC 1005-1006.
43. 15 USC 1693.
44. 18 USC 1341; and 18 USC 1343.
45. 18 USC 1341.
46. 18 USC 1001; and 18 USC 912.
47. 42 USC 2000.
48. OSI Guide, 11; see also DOJ Guide, part V, section B.
49. OSI Guide, attachment 1.1.
50. See, for example, *Warden v. Hayden,* 387 US 294 (1967).
51. *The Rome Labs Incident*: "In March and April 1994, a British hacker known as 'Datastream Cowboy' and another hacker called 'Kuji' (hackers commonly use nicknames or 'handles' to conceal their real identities) attacked Rome Laboratory's computer system over 150 times. To make tracing their attacks more difficult, the hackers wove their way through international phone switches to a computer modem in Manhattan. The two hackers used fairly common hacker techniques, including loading 'Trojan horses' and 'sniffer' programs, to break into the lab's systems. They took control of the lab's network, ultimately taking all 33 subnetworks off-line for several days." The Air Force could not determine whether any of the attacks were a threat to national security in that case. It is quite possible that at least one of the hackers may have been working for a foreign country interested in obtaining military research data or learning exactly what projects the Air Force was working on at the time. "During the attacks, the hackers stole sensitive air tasking order research data . . . [and] also launched other attacks from the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and Defense contractors around the country." The 16-year-old Datastream Cowboy was caught by Scotland Yard authorities last year, and 21-year-old Kuji was apprehended in June of 1996. (See Testimony of Jack L. Brock Jr., director, Defense Information and Financial Management Systems Accounting and Information Management Division, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," GAO Committee on Governmental Affairs, US Senate, Permanent Subcommittee on Investigations (GAO/T-AIMD-96-2), 3. *The Argentine Intrusion*: In August of 1995, intrusions into US Navy computer systems were linked to a computer system that was located at Harvard University and was eventually tracked back to Argentina. This criminal investigation crossed several international borders and required cooperation throughout every step with authorities in diverse jurisdictions. It was the first Title 3 "wiretap" search authorization ever issued for a hacker whose identity was not known. The hacker, a 21- year-old university student, was finally apprehended by Argentine authorities, and apparently did not feel that he had committed any type of misconduct. The hacker's father indicated that "these Yankees don't have the slightest idea about security. Who is at fault? We have done nothing here. Obviously the North Americans are not very clear on security of their systems, if a kid from South America can enter them. I would be ashamed to admit it [sic]." The hacker himself bragged, "You can enter into U.S. military computers, into NASA, a million places . . . I got into all the U.S. Navy defence . . . all the submarines" . . . and "it has been nine months since I'm inside that computer. I could erase everything, enter into any sector and erase any kind of information. I haven't done it because I'm not interested to [sic]." ("Argentine Intrusion Investigation," a presentation by US Naval Criminal Investigative Service at the School of Information Warfare and Strategy's Intermediate Information Based Warfare Course (IB9604), 24 July 1996; see also Public Law 90-351, Title III (note that this search authorization was issued, but since trial has not occurred, it has not yet been tested by a court of competent jurisdiction to address the legality of the issuance. Simply because it has been issued does not necessarily guarantee or certify its propriety under domestic or international law). See the *Austin American Statesman* (newspaper), Saturday, 30 March 1996, and Reuters World Service, Buenos Aires, 30 March 1996. (Note that the local Argentine newspapers *Clarin* and *La Republica* both covered this incident in 1995, but the incident was essentially ignored by the US press.)
52. Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995 at the 543d meeting of the Minister's Deputies, Council of Europe, Strasbourg, France.
53. Sir Arnold Duncan, *The Development of International Justice* (New York: New York University Press, 1954), 23–25.
54. See also Finn Seyersted, *United Nations Forces in the Law of Peace and War* (Leyden, Netherlands: A.W. Sijthoff, 1966).
55. The LOAC used to be known as the "Laws of War," but this terminology became inaccurate when it became clear that armed hostilities and military engagements in the absence of a declaration of war were more frequent and more likely. Thus, the LOAC applies to any armed conflict, whether a "war" is declared or not. Gerhard von Glahn, *Law among Nations: An Introduction to Public International Law* (London: Macmillan Company, 1970), 550–51.
56. Capt Maura T. McGowan, in an unpublished study entitled "Law of Armed Conflict" (Colorado Springs, Colo.: United States Air Force Academy, Department of Law), 20, cites *United States v. List et al.* See United Nations War Crimes Commission, *Trials of War Criminals before the Nuremberg Military Tribunals*, vol. XI, *The High Command Case: The Hostage Case* (Washington, D.C.: US Government Printing Office, 1950), 1253–55; and McDonald, 5.
57. Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949, Article 4.
58. McGowan, 3-4 (citing Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949, 6 UST 3316, TIAS No. 3364, 75 UNTS 135, Article 85).
59. McGowan, 6 (citing the Hague Convention No. IV of 1907, Article 29).
60. Von Glahn, 595.
61. Air Force Policy Directive (AFPD) 51-4, *Compliance with the Law of Armed Conflict,* par. 1.6.1.
62. McDonald, 5.
63. Consider that actions taken via computer would thus not be deemed an "armed attack" since they are not "weapons" and may cause damage, but would not involve an act of "violent force," regardless of how destructive the repercussions of the computer activity may be.
64. An example is the winter blizzard of 1995–1996 in New York City that caused many minor violent outbursts or the multistate power outage caused by a fallen tree in the western United States in the fall of 1996.
65. The potential for this approach arose during the author's interview with Ms. Martha J. Stansell-Gamm, Computer Crime Unit, US Department of Justice, Criminal Division, 10 July 1996.
66. Col Phillip Johnson, HQ USAF/JAI, "Primer on Legal Issues in Information Warfare," talking paper, October 1995, 11.
67. Note that this is an LOAC analysis only and does not consider telecommunications laws and criminal laws that would

likely cloud the issue. These are discussed elsewhere in this article.

68. This incident was pervasively covered in contemporary American media. For example, see articles on the raid in *Newsweek* 107 (28 April 1986): 16–36.

69. Aldrich, 7.

70. It is important to note that this logical conclusion is made in view of the LOAC, and does not consider criminal law or satellite treaties that may be violated by such acts. In peacetime, these would be valid limitations upon a nation's response, reprisal, and war-fighting options and would most certainly be contemplated during wartime before any violations were consciously undertaken.

71. Lt Col Richard Marshall, National Security Agency, Fort Meade, Maryland, interviewed by the author, 12 July 1996.

72. Department of the Air Force Intelligence Law outline created for the Air Force Information Warfare Center, prepared by Col Richard A. McDonald, 6; see also The Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Article 8, The Hague, 18 October 1907.

73. McDonald, 7 (citing Senate, *Military Surveillance of Civilian Politics: A Report of the Subcommittee on Constitutional Rights, Committee on the Judiciary,* 93d Cong., 1st sess. (1973), 117.

74. Ibid., 7.

75. Ibid., 8.

76. *Covert action* is defined as an activity of the US government to influence political, economic, or military conditions abroad, where it is intended that the role of the US government will not be apparent or acknowledged publicly. Covert action intended to influence US domestic political process, public opinion, policies, or media is expressly prohibited. See "Memorandum for IW Wargame Participants," J02L7, by Capt Stephen A. Rose, JAGC, US Navy, Staff Judge Advocate, dated 29 January 1996 (hereinafter Wargame Memorandum).

77. 50 USC 413(b).

78. Ibid.

79. Executive Order (EO)12333, United States Intelligence Activities, 4 December 1981.

80. Ibid.; see also *Federal Register* 46 (1981): 59941.

81. Ibid.

82. McDonald, 9.

83. Wargame Memorandum; see also EO 12333 and *Federal Register* 46 (1981): 59941.

84. Wargame Memorandum.

85. Ibid., 9.

86. Ibid., 10.

87. Ibid.

88. Ibid.

89. Ibid.

90. Ibid., 11.

91. Ibid.

92. Ibid.

93. Ibid.

94. See EO12333 and *Federal Register* 46 (1981): 59941, for a more detailed articulation of the specific authority of various agencies to undertake various surveillance activities.

95. Consider this hypothetical: The intruder is the teenage son of a Pentagon official who played on his father's computer without permission while waiting for his parent to return from a meeting. To send a "logic bomb" back from the point of intrusion to the origin could damage a host of DOD computers and could potentially disable the Pentagon's networks. Clearly an automatic response that is harmful to the computer system may not be in the best interests of the United States.

It is well that war is so terrible, or we should get too fond of it.

—Robert E. Lee