AD NUMBER

ADB257057

NEW LIMITATION CHANGE

TO

Approved for public release, distribution unlimited

FROM

Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use; 19 Jun 2000 Other requests shall be referred to DTIC-AI, Belvoir, VA 22060-6218

AUTHORITY

IATAC ltr, 21 Aug 2001

AN ASSESSMENT OF

INTERNATIONAL LEGAL ISSUES

IN

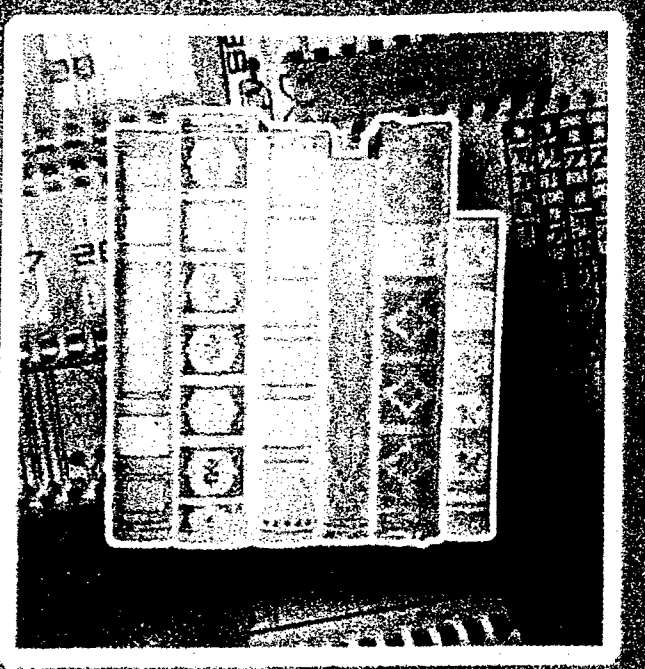
INFORMATION OPERATIONS

MAY 1999

Department of Defense
Office of General Counsel

INFORMATION ASSURANCE COLLECTION ACQUISITIONS

JUNE 2000



IATAC

-mail: iatac@dtic.mil URL: http://iac.dtic.mil/iatac SIPRNET: http://iac.dtic.smil.mil
3190 Fairview Park Drive, Falls Church, VA 22042

ACKNOWLEDGEMENT

This assessment of international legal issues in information operations reflects the combined efforts of a superb team of Department of Defense lawyers. It could not have been produced without the contributions of representatives of the General Counsels of the Army, Navy, Air Force, the National Security Agency and the Defense Information Systems Agency, as well as the Judge Advocates General of the military services and the Legal Counsel to the Chairman of the Joint Chiefs of Staff. Their insight, wisdom and persistence have not only been of great value but have reflected exceeding well on themselves and their offices. The principal draftsman, Phillip A. Johnson (Colonel USAF, Retired), is owed a note of special appreciation; his scholarship and dedication were truly extraordinary.

TABLE OF CONTENTS

I. INTRODUCTION

A. Sources and Application of International Law.

International law consists of binding legal obligations among sovereign states. Two of the basic principles of the international legal system are that sovereign states are legally equal and independent actors in the world community, and that they generally assume legal obligations only by affirmatively agreeing to do so. The most effective instruments in creating international law are international agreements, which may be either bilateral or multilateral. Some of these agreements, such as the United Nations Charter, establish international institutions that the parties agree to invest with certain authority. It is also generally accepted that there is a body of customary international law, which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally obligatory.

International institutions have legislative authority to create legal obligations for nations only when their member nations have agreed to give them that authority. The most prominent example is the power of the UN Security Council to pass resolutions requiring individual nations to perform or refrain from certain actions in order to protect or restore international peace and security in the context of a particular situation. The decisions of the International Court of Justice are binding upon nations that have accepted the jurisdiction of the Court and are parties to litigation before it. Other international institutions can also be given the power to impose binding obligations upon nations that agree to submit to their authority. In addition, certain actions of some international institutions, such as the International Court of Justice and the UN General Assembly, are considered to be persuasive evidence of the existence of principles of customary international law.

As with domestic law, the primary mechanism that makes international law effective is voluntary compliance. Also as with domestic law, the threat of sanctions is often required as well. The international legal system provides institutional enforcement mechanisms such as international litigation before the International Court of Justice and other judicial and arbitral tribunals, as well as the right to petition the United Nations Security Council to authorize coercive measures to protect or restore international peace and security. The international legal system also provides self-help enforcement mechanisms such as the right to use force in individual and collective self-defense and the right in some circumstances to repudiate treaty obligations which have been violated by another party. An aggrieved nation may always withdraw from voluntary relationships involving diplomatic representation and most kinds of commerce. Even the right to publicly complain about another nation's illegal behavior may provide an effective enforcement mechanism if such complaints generate diplomatic costs for the offending nation.

Chief Justice Oliver Wendell Holmes once wrote, "The life of the law has not been logic; it has been experience." It seldom happens that a legislature foresees a problem before it arises and puts into place a legislative solution before it is needed. More typically, legislators react to a problem that has already manifested itself. The international legal system operates in the same manner. The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations.

The development of international law concerning artificial earth satellites provides a good example. If the nations had sat down with perfect foresight and asked themselves, "Should we permit those nations among us that have access to advanced technology to launch satellites into orbit that will pass over the territory of the rest of us and take high-resolution imagery, listen in our telecommunications, record weather information, and broadcast information directly to telephones and computers within our borders?", a very restrictive regime of space law might have resulted. Instead, what happened was that the first satellites launched by the Soviet Union and the United States were seen as entirely benign devices engaged in scientific research, and it was also perfectly clear that no nation had the capability to interfere with them as they passed over its territory. In these circumstances, it quickly became accepted customary international law, soon enshrined in the Outer Space Treaty, that objects in orbit were beyond the territorial claims of any nation, and that outer space is available for exploitation by all.

The history of space law contrasts sharply with that of air law. Much of the early development of heavier-than-air aviation coincided with the First World War, during which the military power of aircraft for intelligence gathering, attacking ground forces, and bombing enemy cities was clearly demonstrated. The result was a highly restricted regime of air law in which any entry into a nation's airspace without its permission was to be regarded as a serious violation of its sovereignty and territorial integrity.

Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.

The actors in the international legal system are sovereign states. International legal obligations and international enforcement mechanisms generally do not apply to individual persons except where a nation enforces certain principles of international law through its domestic criminal law, or in a very limited class of serious offenses (war crimes, genocide, crimes against humanity, and crimes against peace) that the nations have agreed may be tried and punished by international criminal tribunals.

B. Essentials of Treaty Law.

In domestic U.S. law there are important distinctions between treaties and executive agreements. This distinction primarily involves issues of Constitutional authority within the U.S. government, but it is of little importance internationally. Treaties and executive agreements are equally binding between the United States and the other party or parties to an international agreement. We will use the term "treaty" in this paper as a shorthand way of referring to all forms of legally binding state-to-state international agreements.

Treaty obligations are binding on their parties, but international law recognizes certain circumstances in which a nation can regard a treaty obligation as being suspended, modified, or terminated. The parties can always modify or terminate a treaty by mutual consent. Some international agreements expire by their own terms after a fixed period of time. Generally, unless the terms of the agreement establish a right of unilateral withdrawal, a nation may not unilaterally repudiate or withdraw from a treaty unless it has a basis for doing so that is recognized under international law. Treaty obligations are reciprocal in nature. If one of the parties commits a material breach of its obligations under the treaty, the other may be entitled to suspend its own compliance, or to withdraw from the agreement entirely. Also, a fundamental change in circumstances may justify a decision by one of the parties to regard its treaty obligations as suspended or terminated.

One of these fundamental changes of circumstance is the initiation of armed hostilities between the parties. Some international agreements specifically provide that they will remain in effect during armed conflict between the parties, such as law of war treaties and the United Nations Charter. Most treaties, however, are silent on whether or not they will continue to apply during hostilities between the parties. Many peacetime agreements facilitate tourism, transportation, commerce, and other relationships the continuation of which would be fundamentally inconsistent with a state of armed conflict between the parties. Agreements on other subjects, such as boundary settlements and reciprocal rights of inheritance of private property, may be unrelated to the existence of hostilities, and may ultimately be determined to remain in full force. The issues involved may be particularly complicated when the treaty concerned is multilateral, rather than bilateral. When two parties to a multilateral treaty are engaged in armed conflict, the result may well be that the effect of the treaty is suspended between the belligerents, but remains in effect among each belligerent and the other parties. We will see later in this paper that the United States is a party to a variety of bilateral and multilateral agreements containing obligations that may affect information operations. One of our tasks will be to determine as best we can which of these agreements are likely to remain in effect during hostilities. The tests we will apply are (1) whether there is specific language in the treaty addressing its effect during hostilities between the parties, and (2) if there is no such language, whether the object and purpose of the treaty is or is not compatible with a state of armed hostilities between the parties.

C. New Legal Challenges Presented by Information Operations.

Many traditional military activities are included in current concepts of "information operations" and "information warfare," including physical attacks on information systems by traditional military means, psychological operations, military deception, and "electronic warfare" operations such as jamming radar and radio signals. The application of international law to these traditional kinds of operations is reasonably well settled. Similarly, electro-magnetic pulse (EMP) weapons and directed-energy weapons such as lasers, micro-wave devices, and high energy radio frequency (HERF) guns will probably operate in a manner similar enough to that of traditional weapons that one could apply existing legal principles to them without much difficulty. It will not be as easy to apply existing international law principles to **information attack**, a term used to describe the use of electronic means to gain access to or change information in a targeted information system without necessarily damaging its physical components. One of the principal forms of information attack is likely to be **computer network attack**, or in today's vernacular, the "hacking" of another nation's computer systems.

The proliferation of global electronic communications systems and the increased interoperability of computer equipment and operating systems have greatly improved the utility of all kinds of information systems. At the same time, these developments have made information systems that are connected to any kind of network, whether it be the Internet or some other radio or hard-wired communications system, vulnerable to computer network attacks. Moreover, global communications are almost seamlessly interconnected and virtually instantaneous, as a result of which distance and geographical boundaries have become essentially irrelevant to the conduct of computer network attacks. The result is that many information systems are subject to computer network attack anywhere and anytime. The attacker may be a foreign state, an agent of a foreign state, an agent of a non-governmental entity or group, or an individual acting for purely private purposes. The equipment necessary to launch a computer network attack is readily available and inexpensive, and access to many computer systems can be obtained through the Internet or another network to which access is easily obtained.

One major implication is that it may be very difficult to attribute a particular computer network attack to a foreign state, and to characterize its intent and motive. For the purposes of analysis we will initially assume away issues of attribution and characterization, returning to them near the end of the analysis. Another major implication is that an attacker may not be physically present at the place where the effects of the attack are felt. The means of attack may not be tangibly present either, except in the form of anonymous and invisible radio waves or electrons. This will complicate the application of traditional rules of international law that developed in response to territorial invasions and attacks by troops, aircraft, vehicles, vessels, and kinetic weapons that the victim could see and touch, and whose sponsor was usually readily apparent.

II. THE LAW OF WAR

A. Essentials of the Law of War.

The terms "law of war" and "law of armed conflict" are synonymous. The latter term has the virtue that it more clearly applies to all international armed conflicts, whether or not they are formally declared wars. "Law of war" is shorter and more familiar, and we will use it in this

paper. The application of the law of war does not generally depend on which of the parties was at fault in starting the conflict. The law of war applies whenever there is a state of international armed conflict, and it applies in the same manner to all the parties to the conflict. There is a small subset of the law of war that applies to noninternational armed conflicts such as civil wars, but those sorts of conflict are not immediately relevant to this paper and will not be discussed. As with other branches of international law, the law of war is composed of treaties and customary international law. The United States is a party to eighteen law of war treaties, along with their various annexes and protocols, and several more law of war agreements are pending before the Senate. The United States also recognizes the existence of a considerable body of customary law of war.

The general principles of the law of war have been expressed in various ways, but their essence can be said to be as follows:

- Distinction of combatants from noncombatants: With very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy. They must distinguish themselves from noncombatants, and they must not use noncombatants or civilian property to shield themselves from attack. If lawful combatants are captured by the enemy they may not be punished for their combatant acts, so long as they complied with the law of war. They are required to be treated humanely in accordance with agreed standards for the treatment of prisoners of war, and they must be released promptly at the cessation of hostilities. Persons who commit combatant acts without authorization are subject to criminal prosecution.

- Military necessity: Enemy military forces are declared hostile. They may be attacked at will, along with their equipment and stores. Civilians and civilian property that make a direct contribution to the war effort may also be attacked, along with objects whose damage or destruction would produce a military advantage because of their nature, location, purpose, or use. A corollary of this principle is that noncombatants and civilian objects making no direct contribution to the war effort, and whose destruction would provide no significant military advantage to the attacker, are immune from deliberate attack.

- Proportionality: When an attack is made against a lawful military target, collateral injury and damage to noncombatants and civilian property may be unavoidable. Attacks may be carried out against lawful military targets even if some amount of collateral damage is foreseeable, unless the foreseeable collateral damage is disproportionate to the military advantage likely to be attained. The military advantage to be gained from an attack refers to an attack considered as a whole rather than only from isolated or particular parts of an attack. Generally, "military advantage" is not restricted to tactical gains, but is linked to the full context of war strategy. The commander ordering the attack is responsible for making the proportionality judgment. The calculus may be affected somewhat if the enemy has failed to carry out his duty to separate his troops and equipment from noncombatants and civilian property, since in such circumstances the defender must shoulder much of the blame for any collateral damage that results. A corollary of the principle of proportionality is that the attacker has a responsibility to take reasonable steps to find out what collateral damage a contemplated attack may cause.

- Superfluous injury: The nations have agreed to ban certain weapons because they cause superfluous injury. Among these are "dum-dum" bullets, projectiles filled with glass or other nondetectable fragments, poisoned weapons, and laser weapons specifically designed to cause permanent blindness to unenhanced vision.

- Indiscriminate weapons: The nations have agreed to ban certain other weapons because they cannot be directed with any precision against combatants. Among these are bacteriological weapons and poison gas.

- Perfidy: The law of war provides certain visual and electronic symbols to identify persons and property that are protected from attack. Among these are prisoners of war and prisoner of war camps, the wounded and sick, and medical personnel, vehicles, aircraft, and vessels. Any misuse of these protected symbols to immunize a lawful military target from attack constitutes the war crime of perfidy. Suppression of such acts is necessary to preserve the effectiveness of such symbols, since known misuse may lead the combatants to disregard them. For similar reasons, it is unlawful to feign surrender, illness, or death to gain an advantage in combat, as well as to broadcast a false report of a cease-fire or armistice.

- Neutrality: Nations not engaged in a conflict may declare themselves to be neutral. A neutral nation is entitled to immunity from attack by the belligerents, so long as the neutral nation satisfies its obligation not to assist either side. If a neutral nation is unable or unwilling to halt the use of its territory by one of the belligerents in a manner that gives it a military advantage, the other belligerent may have a right to attack its enemy in the neutral's territory. There is considerable support for the argument that the concept of neutrality has no application during a conflict in which one of the belligerents is a nation or coalition of nations authorized by the UN Security Council to use armed force to protect or restore international peace and security. This conclusion is based upon Article 49 of the Charter, which provides, "The Members of the United Nations shall join in affording mutual assistance in carrying out the measures decided upon by the Security Council." In other situations, however, as when a nation uses armed force in individual or collective self-defense without the benefit of a Security Council mandate, it would appear that nations not involved in the conflict retain the option of declaring themselves to be neutral.

B. Application to Information Operations.

It is by no means clear what information operations techniques will end up being considered to be "weapons," or what kinds of information operations will be considered to constitute armed conflict. On the other hand, those issues may not end up being particularly important to the analysis of law of war issues. If the deliberate actions of one belligerent cause injury, death, damage, and destruction to the military forces, citizens, and property of the other belligerent, those actions are likely to be judged by applying traditional law of war principles.

- Distinction of combatants from noncombatants: This rule grew up when combatants could see each other and make a judgment of whether or not to open fire based in part on whether or not the individual in the sights wore an enemy uniform. When the unit of combat came to be a vessel, tank, truck, or aircraft, it became more important that such vehicles be properly marked than that their occupants wear a distinctive uniform. If a computer network attack is launched from a location far from its target, it may be of no practical significance whether the "combatant" is wearing a uniform. Nevertheless, the law of war requires that lawful combatants be trained in the law of war, that they serve under effective discipline, and that they be under the command of officers responsible for their conduct. This consideration argues for retaining the requirement that combatant information operations during international armed conflicts be conducted only by members of the armed forces. If combatant acts are conducted by unauthorized persons, their government may be in violation of the law of war, depending on the circumstances, and the individuals concerned are at least theoretically subject to criminal prosecution either by the enemy or by an international war crimes tribunal. The long-distance and anonymous nature of computer network attacks may make detection and prosecution unlikely, but it is the firmly

established policy of the United States that U.S. forces will fight in full compliance with the law of war.

- Military necessity: In developed nations both military and civilian infrastructures are vulnerable to computer network attacks. During an armed conflict virtually all military infrastructures will be lawful targets, but purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack. Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so. In a long and protracted conflict, damage to the enemy's economy and research and development capabilities may well undermine its war effort, but in a short and limited conflict it may be hard to articulate any expected military advantage from attacking economic targets. Targeting analysis must be conducted for computer network attacks just as it traditionally has been conducted for attacks using traditional weapons.

- Proportionality: During Desert Storm, one of the earliest targets of the coalition bombing campaign was the electrical power system in Baghdad. Considering the important military uses being made of electricity from that system, it was clearly a lawful military target. The Iraqi government then made a public pronouncement that the coalition's attack on the city's electrical power system constituted an act of attempted genocide. The logic of this position was that the city's sewage system depended on electric pumping stations, so when the electricity went out the sewage system backed up and created a threat of epidemic disease. No one took this claim very seriously, but this incident highlights the fact that when an attack is made on an infrastructure that is being used for both military and civilian purposes the commander will not be in a proper position to weigh the proportionality of the expected military advantage against the foreseeable collateral damage unless the commander has made a reasonable effort to discover whether the system is being used for civilian purposes that are essential to public health and safety. This principle operates in exactly the same way whether the attack is carried out using traditional weapons or in the form of a computer network attack.

As stated above, the law of war places much of the responsibility for collateral damage on a defending force that has failed to properly separate military targets from noncombatants and civilian property. When military officials decide to use civilian infrastructure for military purposes (or vice-versa), they ought to consider the fact that such action may make that infrastructure a lawful military target. There may be no choice, as when military traffic has to move on civilian highways and railroads. There may be little alternative to military use of civilian communications systems, since it is impractical to put into place dedicated military communications systems that have sufficient capacity to carry all military communications. Where there is a choice, however, military systems should be kept separate from infrastructures used for essential civilian purposes.

Military command and control systems have long been recognized as lawful military targets. Civilian media generally are not considered to be lawful military targets, but circumstances may make them so. In both Rwanda and Somalia, for example, civilian radio broadcasts urged the civilian population to commit acts of violence against members of other tribes, in the case of Rwanda, or against UN-authorized forces providing humanitarian assistance, in the case of Somalia. When it is determined that civilian media broadcasts are directly interfering with the accomplishment of a military force's mission, there is no law of war objection to using the minimum necessary force to shut them down. The extent to which force can be used for purely psychological operations purposes, such as shutting down a civilian radio station for the sole

purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community.

- Superfluous injury: We are not aware that any weapon or device yet conceived specifically for use in information operations has any potential for causing superfluous injury, but new systems should always be reviewed with an eye to their potential for causing catastrophic and untreatable injuries to human beings to an extent not required by military necessity.

- Indiscriminate weapons: The prohibition on indiscriminate weapons may apply to information operations techniques such as malicious logic, as when malicious logic launched against a military information system spreads to other information systems being used to provide essential services to noncombatants. It might also apply if malicious logic spreads to information systems belonging to neutral or friendly nations. Finally, it might be applied indirectly if the consequence of a computer network attack is to release dangerous forces, such as opening the floodgates of a dam, causing an oil refinery in a populated area to explode in flames, or causing the release of radioactivity.

- Perfidy: It may seem attractive for a combatant vessel or aircraft to avoid being attacked by broadcasting the agreed identification signals for a medical vessel or aircraft, but such actions would be a war crime. Similarly, it might be possible to use computer "morphing" techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this would also be a war crime.

- Neutrality: If a neutral nation permits its information systems to be used by the military forces of one of the belligerents, the other belligerent generally has a right to demand that it stop doing so. If the neutral refuses, or if for some reason it is unable to prevent such use by an belligerent, the other belligerent may have a limited right of self-defense to prevent such use by its enemy. It is quite foreseeable, for example, that a belligerent might demand that a neutral nation not provide satellite imagery of the belligerent's forces to its enemy, or that the neutral cease providing real-time weather information or precision navigation services.

There appears, however, to be a limited exception to this principle for communications relay systems. The primary international agreement concerning neutrality, the 1907 *Hague Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*, to which the United States is a party, provides in Articles 8 and 9 that "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 telegraph apparatus belonging to it or to Companies or private individuals," so long as such facilities are provided impartially to both belligerents. The plain language of this agreement would appear to apply to communication satellites as well as to ground-based facilities.

There is nothing in this agreement, however, that would suggest that it applies to systems that generate information, rather than merely relay communications. These would include the satellite imagery, weather, and navigation systems mentioned above, as well as other kinds of intelligence-producing systems such as signals intelligence and hydrophonic systems. For example, if a belligerent nation demanded that the U.S. government deny GPS navigation services to its enemy, and if the U.S. were unable or unwilling to comply, the belligerent may have the right to take necessary and proportional acts in self-defense, such as jamming the GPS signal in the combat area.

International consortia present special problems. Information systems built around space-based components require such huge investments and access to such advanced technology that even developed nations prefer to share the costs with other nations. Where an international communications system is developed by a military alliance such as NATO, few neutrality issues are likely to arise. Other international consortia, however, provide satellite communications and weather data that are used for both civilian and military purposes, and they have a breath of membership that virtually guarantees that not all members of the consortium will be allies in future conflicts. Some current examples are INTELSAT, INMARSAT, ARABSAT, EUTELSAT, and EUMETSAT.

The members of some these consortia have attempted to deal with the possibility that one or more of the member nations will be involved in an armed conflict by limiting the use that may be made of the system during armed conflict. The INMARSAT agreement, for example, provides that the mobile communications service provided by the system may be used "exclusively for peaceful purposes." This provision provides less than a perfect solution, however, since the member nations and the INMARSAT staff have concluded that this language permits use of INMARSAT by UN peacekeeping or peacemaking forces acting under the auspices of the UN Security Council, even if they are engaged in armed conflict to accomplish their missions.

C. Assessment. There are novel features of information operations that will require expansion and interpretation of the established principles of the law of war. Nevertheless, the outcome of this process of extrapolation appears to be reasonably predictable. The law of war is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations.

III. INTERNATIONAL LEGAL REGULATION OF THE USE OF FORCE IN "PEACETIME"

A. International Law Concerning the Use of Force among Nations.

As discussed above, the law of war authorizes a nation engaged in an international armed conflict to employ armed force to attack lawful military targets belonging to the enemy. Resolutions of the United Nations Security Council (UNSC) may also authorize the use of armed force as provided in the UN Charter. The focus of this section, however, is on the application of international law principles in circumstances where there is neither a state of armed conflict nor a UNSC mandate – i.e., in peacetime, including the conduct of military operations other than war.

An exploration of the manner in which international law on the use of force among nations is likely to apply to peacetime computer intrusions will serve three distinct purposes: (1) it will enable a government that is resolved to conduct itself in scrupulous compliance with international law to avoid activities that are likely to be regarded by the target nation and the world community as violations of international law; (2) it will enable a government contemplating activities that might be considered to violate international law to weigh the risks of such actions; and (3) it will enable a government that is the victim of an information attack to identify the remedies afforded to it by international law, including appeals to the Security Council, the use of force in self-defense, and other self-help remedies not involving the use of force.

The frequently-heard question, "Is a computer network attack an **act of war**?" invokes an obsolete concept not mentioned in the UN Charter and seldom heard in modern diplomatic discourse. An act of war is a violation of another nation's rights under international law that is so egregious that the victim would be justified in declaring war. Declarations of war have fallen into disuse, and the act of war concept plays no role in the modern international legal system. In any event, significant sanctions may follow from much less serious violations of another nation's rights that would not be regarded as acts of war.

The members of the United Nations have agreed in Article 2 (4) of the UN Charter to "refrain in their international relations from **the threat or use of force** against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

This obligation is elaborated in the *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*, General Assembly Resolution 2625 (1970), which provides in part:

- "A **war of aggression** constitutes a crime against the peace for which there is responsibility under international law."

- "States have a duty to refrain from **acts of reprisal involving the use of force**."

- "Every State has the duty to refrain from **organizing, instigating, assisting or participating in acts of civil strife or terrorist acts** in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, **when the acts referred to in the present paragraph involve a threat or use of force**."

- "Nothing in the foregoing paragraphs shall be construed as enlarging or diminishing in any way the scope of the provisions of the Charter concerning cases in which the use of force is lawful."

NOTE: The United States has often expressed the view that most General Assembly resolutions are only recommendations, but that in exceptional cases particular General Assembly resolutions that are meant to be declaratory of international law, are adopted with the support of all members, and are observed by the practice of states, are persuasive evidence of customary international law on a particular subject. Representatives of the United States have on several occasions publicly endorsed the Declaration on Friendly Relations as one of the few General Assembly resolutions that the United States regards as an authoritative restatement of customary international law, at least until the practice of states fails to demonstrate that they consider its principles to be legally binding.

In its 1974 "Definition of Aggression" Resolution, the General Assembly further provided:

- Article 1. **Aggression** is the **use of armed force** by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.

- Article 2. The **first use of armed force** by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

- Article 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of Article 2, qualify as an **act of aggression**:
  (a) The **invasion or attack by the armed forces** of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any **annexation by the use of force of the territory** of another State or part thereof;
  (b) **Bombardment by the armed forces** of a State against the territory of another State or the **use of any weapons** by a State **against the territory** of another State;
  (c) The **blockade of the ports or coasts** of a State **by the armed forces** of another State;
  (d) An **attack by the armed forces** of a State **on the land, sea or air forces, or marine and air fleets** of another State;
  (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
  (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
  (g) The **sending** by or on behalf of a State **of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force** against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

NOTE: The United States delegation noted that the text of this resolution reflected hard bargaining among the 35 states that were members of the Special Committee on the Question of Defining Aggression. After the resolution was adopted by the General Assembly without a vote,

the U.S. delegation stated the view that the resolution did not establish rights and obligations of states, but that it was "likely to provide useful guidance" to the Security Council. Translated, this statement appears to indicate that the United States does not regard the language of this resolution as a completely authoritative restatement of customary international law, but that its essential concepts are correct. In any event, the question of what constitutes an "act of aggression" is unlikely to be as useful for our purposes as is the question, what kinds of information attacks are likely to be considered by the world community to be "armed attacks" and "uses of force."

Turning to the question of when force may lawfully be used by nations, the United Nations Charter provides that in some circumstances the Security Council may authorize the use of coercive measures, including military force:

- Article 39. The Security Council shall determine the existence of any **threat to the peace, breach of the peace, or act of aggression** and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

- Article 41. The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

- Article 42. Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

Perhaps most significantly, the Charter also provides in Article 51, "Nothing in the present Charter shall 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 measures necessary to maintain international peace and security."

Read together, these provisions of the Charter and the related General Assembly resolutions provide a myriad of terms and concepts concerning prohibited uses of force among nations, including the threat or use of force, acts of aggression, wars of aggression, the use of armed force, acts of armed force, invasion, attack, bombardment, and blockade. These acts may be directed at the victim nation's territorial integrity or political independence, or against its military forces or marine or air fleets. They all have in common the presence of troops and the use of traditional military weapons. The question before us is how they are likely to apply to computer network attacks.

Further, when one looks for provisions describing a sanction or remedy, only two provisions present themselves: the authority of the Security Council to authorize various sanctions, including the use of the members' armed forces, when it finds there is a "threat to the peace, breach of the peace, or act of aggression;" and Article 51's recognition of the inherent right of self defense "if an armed attack occurs."

There is no requirement that a "threat to the peace" take the form of an armed attack, a use of force, or any other condition specified in the charter. The Security Council has the plenary

authority to conclude that virtually any kind of conduct or situation constitutes a "threat to the peace" in response to which it can authorize remedial action of a coercive nature. Nothing would prevent the Security Council from finding that a computer network attack was a "threat to the peace" if it determined that the situation warranted such action. It seems unlikely that the Security Council would take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council. The debate in such a case would more likely center on the offender's intent and the consequences of the offending action than on the mechanism by which the damage was done.

The language of Article 51, on the other hand, requires an "armed attack." A close parsing of the language would tend to limit its effect to attacks and invasions using traditional weapons and forces. On the other hand, there is a well-established view that Article 51 did not create the right of self-defense, but that it only recognized a pre-existing and inherent right that is in some respects broader than the language of Article 51.

History has also seen the emergence of such derivative doctrines as "anticipatory self-defense" and "self-defense in neutral territory," both of which have been relied upon by the United States in certain circumstances. "Anticipatory self-defense" permits a nation to strike the first blow if it has good reason to conclude that it is about to be attacked. The JCS Standing Rules of Engagement implement this doctrine in their authorization of the use of force in response to a demonstration of "hostile intent" by an adversary. "Self-defense in neutral territory" is the right to use force to neutralize a continuing threat located in the territory of a neutral state, but not acting on its behalf, when the neutral state is unable or unwilling to execute its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation. This doctrine has venerable roots in U.S. foreign and defense policy, dating at least to the *Caroline* incident. In December 1837, Canada, which was still a British colony, was fighting an insurrection. More than 1,000 insurgents were encamped on both the Canadian and U.S. sides of the Niagara River. A small steamer, the *Caroline*, was used by the insurgents to travel across and along the river. On the night of December 19, 1837, a party of British troops crossed the Niagara and attacked the *Caroline* in the port of Schlosser, New York, setting the vessel on fire and casting it adrift over the Niagara Falls. One U.S. citizen was killed on the dock, another was missing, and several others were wounded. The United States demanded reparations. The British Government responded that it had acted in self-defense. Secretary of State Daniel Webster agreed that the doctrine of self-defense in neutral territory was a valid principle of international law, but asserted that it did not apply in the circumstances of this case. Britain continued to maintain that its action was legal, but nonetheless apologized for the invasion of U.S. territory. No reparations were paid.

In 1986 the United States bombed Libya as a response to Libya's continuing support for terrorism against U.S. military forces and other U.S. interests. In June 1993 U.S. forces attacked the Iraqi military intelligence headquarters because the government of Iraq had conspired to assassinate former President Bush. In August 1998 U.S. cruise missiles struck a terrorist training camp in Afghanistan and a chemical plant in Sudan in which chemical weapons had been manufactured. The rationale articulated for each of these actions was self-defense. Acts of self-defense must satisfy the tests of necessity and proportionality, but there is no requirement that an act of self-defense use the same means as the provocation, that the object of the attack be either a similar type of target or the means used in the offending attacks, or that the action taken be contemporaneous with the provocation, particularly if the attacker is responding to a continuing course of conduct.

B. Acts not Amounting to the Use of Force.

In its 1949 decision in the Corfu Channel Case, the ICJ ruled that the intrusion of British warships into Albanian territorial waters, which it found to have been without justification under any principle of international law, constituted a violation of Albania's territorial sovereignty. The result seems to be recognition of a general international law of trespass, although the remedy may be limited to a declaratory judgment that the victim's rights have been violated.

The ICJ's predecessor, the Permanent Court of International Justice, in its 1928 Chorzow Factory Decision, declared that reparations were due to any nation whose rights under international law were violated by another nation. This concept is often referred to as the doctrine of state responsibility.

There is also a general recognition of the right of a nation whose rights under international law have been violated to take **countermeasures** against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force. For example, an arbitral tribunal in 1978 ruled that the United States was entitled to suspend French commercial air flights into Los Angeles after the French had suspended U.S. commercial air flights into Paris. Discussions of the doctrine of countermeasures generally distinguish between countermeasures that would otherwise be violations of treaty obligations or of general principles of international law (in effect, reprisals not involving the use of armed force) and retorsions – actions that may be unfriendly or even damaging, but which do not violate any international legal obligation. The use of countermeasures is subject to the same requirements of necessity and proportionality as apply to self-defense. Some examples of countermeasures that have been generally accepted as lawful are the suspension of diplomatic relations, trade and communications embargoes, cutting off foreign aid, blocking assets belonging to the other nation, and prohibiting travel to or from the other nation.

The international law doctrines of self-defense, reprisal, and countermeasures all require that a nation invoking them do so with the intent of protecting itself against further harm, either by directly blocking further hostile acts against itself or by persuading its tormentor to cease and desist. The motive must be protection of the nation or its citizens or other national interests from further harm – the satisfaction of extracting revenge, by itself, is not acceptable. These doctrines also demand that a state do only what is necessary and proportional in the circumstances.

In summary, it appears that one trend in international law is to provide some kind of remedy for every violation of a nation's rights under international law. Some of these remedies are in the nature of self-help, such as armed self-defense, the interruption of commercial or diplomatic relations, or public protest. Other remedies may be sought from international institutions, such as an imposition of coercive measures by the Security Council, or a declaratory judgment or an order to make reparations from an international tribunal. The issue for the victim is to choose the most effective available sanction. The issue for a nation contemplating an action that may be considered to violate the rights of another nation under international law is to accurately predict what sanctions such action may provoke.

C. Application to Computer Network Attacks.

There is no way to be certain how these principles of international law will be applied by the international community to computer network attacks. As with other developments in

international law, much will depend on how the nations and international institutions react to the particular circumstances in which these issues are raised for the first time. If we were to limit ourselves to the language of Article 51, the obvious question would be, "Is a computer network attack an 'armed attack' that justifies the use of force in self-defense?" If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism. It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.

If the international community were persuaded that a particular computer network attack or a pattern of such attacks should be considered to be an "armed attack," or equivalent to an armed attack, it would seem to follow that the victim nation would be entitled to respond in self-defense either by computer network attack or by traditional military means in order to disable the equipment and personnel that were used to mount the offending attack. In some circumstances it may be impossible or inappropriate to attack the specific means used in an attack (e.g. because the specific equipment and personnel used cannot be reliably identified or located, or an attack on the specific means used would not be effective, or an effective attack on the specific means used might result in disproportionate collateral damage). Where the specific means cannot be effectively attacked, any legitimate military target could be attacked, including intelligence and military leadership targets, as long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to undertake them.

There has been some support for the proposition that a nation has an inherent right to use force in self-defense against acts that do not constitute a classic armed attack. This view is supported by the inclusion in the General Assembly's definition of aggression of acts that do not entail armed attacks by a nation's armed forces, such as the unlawful extension of the presence of visiting forces, or allowing a nation's territory to be used by another state "for perpetrating an act of aggression against a third State." (See pages 14-15 above). U.S. practice also support this position, as demonstrated in the 1986 bombing of Libyan command and leadership targets to persuade Libya to stop sponsoring terrorist attacks against U.S. interests, and in the 1998 attack on the Iraqi military intelligence headquarters to persuade Iraq to desist from assassination plots against former President Bush. A contrary view was expressed in the International Court of Justice's 1986 ruling in Nicaragua v. U.S. that the provision of arms by Nicaragua to the leftist rebels in El Salvador did not constitute an armed attack on El Salvador, so it could not form the basis of a collective self-defense argument that would justify armed attacks in response, such as laying of mines in Nicaraguan waters or certain attacks on Nicaraguan ports, oil installations and a naval base – acts that were "imputable" to the United States. The Court also said it had insufficient evidence to determine whether certain cross-border incursions by Nicaraguan military forces into the territory of Honduras and Costa Rico constituted armed attacks. The extent to which Nicaragua's conduct would justify El Salvador and its ally the United States in responding

in ways that did not themselves constitute an armed attack was not before the Court. The opinion of the court nevertheless provides some support for the proposition that the provocation must constitute an armed attack before it will justify an armed attack in self-defense. It seems safe to say that the issue of whether traditional armed force may be used in self-defense in response to provocations that are not technically regarded as armed attacks is far from settled, and that the positions taken by states may be sharply influenced by the nature of the events concerned, together with all attendant policy and political considerations.

By logical implication, to the extent that a nation chooses to respond to a computer network attack by mounting a similar computer network attack of its own, the issue of whether the initial provocation constituted an armed attack may become a tautology. If the provocation is considered to be an armed attack, the victim may be justified in launching its own armed attack in self-defense. If the provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack. Accordingly, the question of the availability of the inherent right of self-defense in response to computer network attacks comes into sharpest focus when the victim of a computer network attack considers acting in self-defense using traditional military means. The issue may also arise if the response causes disproportionately serious effects (e.g., if a state responded to a computer network attack that caused only minor inconvenience with its own computer network attack that caused multiple deaths and injuries). As in all cases when a nation considers acting in self-defense, the nation considering such action will have to make its best judgment on how world opinion, or perhaps a body such as the International Court of Justice (ICJ) or the UNSC, is likely to apply the doctrine of self-defense to electronic attacks. As with many novel legal issues, we are likely to discover the answer only from experience.

It seems beyond doubt that any unauthorized intrusion into a nation's computer systems would justify that nation at least in taking self-help actions to expel the intruder and to secure the system against reentry. An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community. Furthermore, the act of obtaining unauthorized access to a nation's computer system creates a vulnerability, since the intruder will have had access to the information in the system and he may have been able to corrupt data or degrade the operating system. Accordingly, the discovery that an intrusion has occurred may call into question the reliability of the data and the operating system and thus reduce its utility. If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community.

D. An "Active Defense" against Computer Network Attacks.

A persistent foreign intruder who gains repeated unauthorized entry into a nation's computer systems by defeating a variety of security measures or who gains entry into a number of computer systems may demand a different response. Such behavior may indicate both that there is a continuing danger and that coercive measures are necessary to stop the intruder's pattern of conduct. Similarly, there may be a right to use force in self defense against a single foreign electronic attack in circumstances where significant damage is being done to the attacked system

or the data stored in it, when the system is critical to national security or to essential national infrastructures, or when the intruder's conduct or the context of the activity clearly manifests a malicious intent.

If it is capable of doing so, in such circumstances the victim nation may be justified in launching a computer attack in response, intended to disable the equipment being used by the intruder. Disabling one computer may or may not defeat a state-sponsored operation. It may, however, serve as a "shot across the bow" warning of more serious consequences if the offending behavior continues. It is also an action unlikely to come to public attention unless one of the two governments announces it, making it a potentially useful measure for conflict avoidance. Conducting a responsive computer network attack as a measure of self-defense against foreign computer network attacks would have the major advantage that it would minimize issues of proportionality, which would be more likely to arise if traditional military force were used, such as firing a cruise missile at the building from which a computer network attack is being conducted. Either response would likely be analyzed on the basis of the traditional criteria of necessity and proportionality.

If it is impractical to focus an attack on the equipment used in the provocation, any legitimate military target may be attacked. The primary value of being able to demonstrate a nexus between the provocation and the response is to be able to argue the likely therapeutic effect of the force used in self-defense. As a practical matter, the next most attractive target after the equipment used in the provocation may be the offending nation's communications systems, or its military or intelligence chain of command. The consequences of a large-scale campaign of computer network attacks might well justify a large-scale traditional military response. A Russian academic took this argument to its extreme in a published statement to the effect that Russia reserves the right to respond to an information warfare attack with nuclear weapons.

As stated above, the discussion up to this point has assumed we know who an intruder is, and that we are confident in characterizing his intent. In practice, this is seldom the case, at least in the early stages of responding to computer intrusions. The above legal analysis may change if the identity and location of an intruder is uncertain, or if his intent is unclear.

Identification of the originator of an attack has often been a difficult problem, especially when the intruder has used a number of intermediate relay points, when he has used an "anonymous bulletin board" whose function is to strip away all information about the origin of messages it relays, or when he has used a device that generates false origin information. Progress has been made, however, in solving the technical problem of identifying the originator of computer messages, and reliable identification of the computer that originated a message may soon be routinely available. Attribution may also be provided by intelligence from other sources, or it might be reliably inferred from the relationship of the attack to other events.

Locating the computer used by the intruder does not entirely solve the attribution problem, however, since it may have been used by an unauthorized person, or by an authorized user for an unauthorized purpose. A parent may not know that the family computer is being used for unlawful attacks on government computer systems. Universities, businesses, and other government agencies may be similarly unaware that their computer systems are being misused. The owner of a computer system may have some responsibility to make sure it is not being used for malicious purposes, but the extent of such responsibility, and the consequences of failing to meet it, have apparently not been addressed in any U.S. or foreign statute or court decision. These considerations should make us cautious in implementing any "active defense" system for government computer systems. Nevertheless, circumstances may arise in which the urgency of

protecting critical information systems from serious damage may warrant adoption of a properly designed "active defense."

Similarly, characterization of an intruder's intentions may be difficult. Nevertheless, such factors as persistence, sophistication of methods used, targeting of especially sensitive systems, and actual damage done may persuasively indicate both the intruder's intentions and the dangers to the system in a manner that would justify use of an "active defense." As with attribution, there may be useful intelligence on this issue from other sources, or it may be possible to reliably infer the intent of the intruder from the relationship of the attack to other events.

A determination that an intrusion comes from a foreign country is only a partial solution to the attribution problem, since the attack may or may not be state-sponsored. State-sponsored attacks may well generate the right of self-defense. State sponsorship might be persuasively established by such factors as signals or human intelligence, the location of the offending computer within a state-controlled facility, or public statements by officials. In other circumstances, state sponsorship may be convincingly inferred from such factors as the state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks.

Attacks that cannot be shown to be state-sponsored generally do not justify acts of self-defense in another nation's territory. States jealously guard their sovereign prerogatives, and they are intolerant of the exercise of military, law-enforcement, and other "core sovereign powers" by other states within their territory without their consent. When individuals carry out malicious acts for private purposes against the interests of one state from within the territory of a second state, the aggrieved state does not generally have the right to use force in self-defense against either the second state itself or the offending individual. Even if it were possible to conduct a precise computer network attack on the equipment used by such individual actors, the state in which the effects of such an attack were felt, if it became aware of it, could well take the position that its sovereignty and territorial integrity had been violated. The general expectation is that a nation whose interests are damaged by the private conduct of an individual who acts within the territory of another nation will notify the government of that nation and request its cooperation in putting a stop to such conduct.

Only if the requested nation is unwilling or unable to prevent recurrence does the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation. The U.S. cruise missile strikes against terrorists camps in Afghanistan on 20 August 1998 provides a close analogy in which the United States attacked camps belonging to a terrorist group located in the territory of a state which had clearly stated its intention to continue to provide a refuge for the terrorists. At some point, providing safe refuge for those who conduct attacks against another nation becomes complicity in those attacks. At a minimum, the offended nation is authorized to attack its tormenters, the terrorists. As complicity shades into the kinds of active support and direction that are commonly called "state sponsorship," military and leadership targets of the host state may themselves become lawful targets for acts of self-defense.

Attacks on insurgents or on terrorists and other criminals using a neutral nation's territory as a refuge may also be justified when the neutral state is unable to satisfy its obligations. During the Vietnam war, the United States attacked North Vietnamese military supply lines and base camps in Cambodia after the Cambodian government took the position that it was unable to prevent North Vietnam from making such use of its territory. This principle might justify using

active defense measures against a computer intruder located in a neutral nation if the government of the neutral nation declared it had no way to locate the intruder and make him stop, or if its behavior made it clear that it could not or would not act, or even if the circumstances did not allow time for diplomatic representations to be effective. As an analogy, it seems unlikely that a nation would complain very loudly if its neighbor nation returned fire against a terrorist sniper firing from its territory.

In summary, the international law of self-defense would not generally justify acts of "active defense" across international boundaries unless the provocation could be attributed to an agent of the nation concerned, or until the sanctuary nation has been put on notice and given the opportunity to put a stop to such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile. Nevertheless, in some circumstances the National Command Authority (NCA) might decide to defend U.S. information systems by attacking a computer system overseas, and take the risk of having to make an apology or pay compensation to the offended government. Among the factors the NCA would probably consider would be the danger presented to U.S. national security from continuing attacks, whether immediate action is necessary, how much the sanctuary nation would be likely to object, and how the rest of the world community would be likely to respond.

There need be less concern for the reaction of nations through whose territory or communications systems a destructive message may be routed. If only the nation's public communications systems are involved, the transited nation will normally not be aware of the routing such a message has taken. Even if it becomes aware of the transit of such a message and attributes it to the United States, there would be no established principle of international law that it could point to as being violated. As discussed above, even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft.

A transited state would have somewhat more right to complain if the attacking state obtained unauthorized entry into its computer systems as part of the communications path to the target computer. It would be even more offended if malicious logic directed against a target computer had some harmful effect against the transited state's own equipment, operating systems, or data. The possibility of such collateral damage would have to be carefully considered by the state launching any such attack. If there were a high potential for such collateral damage to transited systems, the weapon might even be considered to be an "indiscriminate" weapon incapable of being reliably directed against a legitimate target.

There are at least two ways in which the availability of improved technology may affect the active-defense equation. First, it might be argued that as a government acquires the ability to build better firewalls and other security systems it will be harder to argue that an active defense is "necessary." This argument might be raised even if the target government has failed to install all possible technological security measures on the system that is under attack. This demanding approach to "necessity" finds little support in the practice of nations. The focus of self-defense analysis is on events as they unfold, and not as they might have been if different budgeting and acquisition decisions had been made sometime in the past. If such systems are in place, however, their apparent effectiveness should be taken into account in deciding whether active defense measures

are necessary. This does not mean that a nation has no right of self-defense where a first attempted intrusion fails, or even when a series of intrusions fail. If an attacker is permitted to continue mounting a campaign of such attacks it may learn by trial and error, it may employ other capabilities, or it may stumble onto a point of vulnerability. Just as an infantry unit exercising the right of self-defense may pursue a force that breaks off an attack and attempts to retreat until the attacker ceases to be a threat, decisions on taking measures of self-defense against computer network attacks must take into account the extent to which an attacker continues to present a threat of continuing attacks.

Another possible implication of a defender's technological prowess may arise when a nation has the capacity for graduated self-defense measures. Some may argue that a nation having such capabilities must select a response that will do minimal damage. This is a variant of the argument that a nation possessing precision-guided munitions must always use them whenever there is a potential for collateral damage. That position has garnered little support among nations and has been strongly rejected by the United States. There is broad recognition that the risk of collateral damage is only one of many military considerations that must be balanced by military authorities planning an attack. One obvious consideration is that a military force that goes into a protracted conflict with a policy of always using precision-guided munitions whenever there is any potential for collateral damage will soon exhaust its supply of such munitions. Similarly, military authorities must be able to weigh all relevant military considerations in choosing a response in self-defense against computer network attacks. These considerations will include the probable effectiveness of the means at their disposal, the ability to assess their effects, and the "fragility" of electronic means of attack (i.e., once they are used, an adversary may be able to devise defenses that will render them ineffective in the future). In the process of reasoning by analogy to the law applicable to traditional weapons, it must always be kept in mind that computer network attacks are likely to present implications that are quite different from the implications presented by attacks with traditional weapons. These different implications may well yield different conclusions.

It may be possible to specify certain information systems that are vital to national security – both government systems and key civilian infrastructure systems. This process should serve both to give such systems high priority for security measures and also to identify a class of systems any attack on which would immediately raise the issue of whether an active defense should be employed. This should not, of course, eliminate consideration of using an active defense against attacks on systems not on such a "vital systems" list where the circumstances justify such action. For example, a vigorous attack that threatens to overwhelm an information system not on the "vital systems" list but that performs an important national security function could be a more valid occasion to use active defense measures than would be a trivial and easily defeated attack on a designated "vital system." A list of "vital systems" would serve primarily as a alert mechanism that would bring about a prompt high-level evaluation of all the circumstances.

In addition, it would be useful to create a process for determining when the response to a computer intrusion should shift from the customary law enforcement and counter-intelligence modes to a national defense mode. Such a process should include (1) a statement of general criteria to be applied; (2) identification of officials or agencies that will be involved in making the decision; and (3) procedures to be followed.

There are of course a variety of treaty obligations that will have to be considered before adopting an "active defense" against foreign computer network attacks, and these will be discussed below. There are also a variety of domestic legal concerns that will have to be

addressed, and these will be discussed in the companion assessment of domestic law issues in information operations.

E. Assessment. It is far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or "uses of force," and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms. The most likely result is an acceptance that a nation subjected to a state-sponsored computer network attack can lawfully respond in kind, and that in some circumstances it may be justified in using traditional military means in self-defense. Unless the nations decide to negotiate a treaty addressing computer network attacks, which seems unlikely anytime in the near future, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period.

IV. SPACE LAW

A. Introduction

International law regulating activities in outer space is important to the information operator because space segments are critical to so many important information systems. These systems perform such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence. In fact, it can be said that at the current stage of space activity, the exclusive functions of both military and civilian satellites are to gather and relay information. In the conduct of information operations, there will be strong imperatives to interfere with the space-based information systems belonging to an adversary, and to defend one's own.

One approach to attacking space systems is by targeting their ground stations. Another approach is to jam or "spoof" their communications links. Such actions are subject to the normal international law principles governing other terrestrial activity. Sometimes, however, it may be more effective to attack the satellite or satellites that form the space segment of the system. As we will see, activities in space are subject both to general principles of international law and to a number of treaty obligations that apply specifically to space activities.

B. Space Law Treaties

There is probably no other field of human endeavor that produced so much international law in such a short period. Within twenty years after the first Sputnik launch in 1957, international diplomatic conferences produced four major widely-accepted multilateral space law treaties. Taken together, these treaties provide the foundations of existing space law.

- *The Treaty on Principles Governing the Activities of States in the Exploration and Use Of Outer Space, including the Moon and Other Celestial Bodies* (the Outer Space Treaty, 1967)

- *The Agreement on the Rescue of Astronauts, Return of Astronauts, and the Return of Objects Launched into Outer Space* (the Rescue and Return Agreement, 1968)

- *The Convention on International Liability for Damages Caused by Space Objects* (the Liability Convention, 1972)

- *The Convention on the Registration of Objects Launched into Outer Space* (the Registration Convention, 1975)

Note: There is another treaty called the Moon Agreement of 1979 which the United States has never signed and which has attracted only 9 parties, among whom only France is active in space operations. In addition, several provisions of the 1980 Environmental Modification Convention apply to space activity. These agreements are not directly relevant to information operations, however, and they will not be discussed further here.

The four major space treaties together establish the following principles that are directly relevant to information operations. These principles have been so widely accepted that they are generally regarded as constituting binding customary international law, even for non-parties to these agreements.

- Space is free for exploration and use by all nations. It is not subject to national appropriation by claim of sovereignty, use, occupation, or any other means.
- Activities in space shall be conducted with due regard for the interests of other states.

- States that launch space objects are liable for any damage they may do in space, in the air, or on the surface of the Earth. Different standards of liability are established for damage done to other items in space, for which a "fault" standard applies, and damage done on the surface of the Earth and to aircraft in flight, for which absolute liability applies.

- Space activities are subject to general principles of international law, including the UN Charter.

Several conclusions are apparent from these general principles. The first is that the rules on the use of force discussed in Section III of this paper apply fully to activities in outer space. Among these are that nations are obliged not to use force in their relations with each other unless they are acting in self-defense or when authorized to do so by the UN Security Council. Once again, however, as with other forms of information operations, one has to consider what actions by or against objects in space will be considered to be uses of force. The world community would probably not hesitate to regard as a use of force the destruction of a satellite by a missile or a laser. It would probably react similarly if it could be proven that one nation took over control of another nation's satellite by electronic means and caused it to fire its retro rockets and fall out of orbit. In such a case, the consequences will probably matter more than the mechanism used. The reaction of the world community to lesser kinds of interference is hard to predict. For example, if one nation were able by electronic means to suspend the operations of another nation's satellite for a brief period, after which it returned to service undamaged, it seems likely that the world community would consider such action as a breach of the launching nation's sovereign rights, but not as a use of armed force.

One could argue, however, that this argument is unimportant because the space treaties create a specific obligation not to interfere with the space activities of other nations, and to pay reparations for any damages resulting from such interference. This argument appears to have considerable force, at least in peacetime. During an international armed conflict between the two nations concerned, however, the law of armed conflict would apply unless it was trumped by the principle of noninterference with space systems. Resolution of this issue depends largely on whether the four space treaties will be considered to apply during an armed conflict. None of them has any specific provision that indicates whether the parties intended that the agreement apply in wartime.

There appears to be a strong argument that the principle of noninterference established by these agreements is inconsistent with a state of hostilities, at least where the systems concerned are of such high military value that there is a strong military imperative for the adversary to be free to interfere with them, even to the extent of destroying the satellites in the system. As indicated in the discussion of treaty law in the introduction to this paper, the outcome of this debate may depend on the circumstances in which it first arises in practice. Nevertheless, it seems most likely that these agreements will be considered to be suspended between the belligerents for the duration of any armed conflict, as least to the extent necessary for the conduct of the conflict.

If the principle of noninterference is regarded as suspended for the period of the conflict, it also seems likely that the liability provisions in these agreements would also be suspended, at least between the parties. This would not, however, excuse the belligerents from liability to neutral nations if their actions caused damage to their citizens or property

C. Specific Prohibitions of Military Activities in Space

There is a popular notion that military activities in space are prohibited – that space is a place a little closer to heaven into which the nations have agreed not to introduce weapons and human conflict. There is a germ of truth in this notion, supported by high flights of rhetoric in international fora, but the existing treaty restrictions on military operations in space are in fact very limited. These restrictions are included in both the space treaties listed above and in various arms control agreements.

The Outer Space Treaty provides that the parties will not "place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies [i.e., the moon, planets, and asteroids], or station such weapons in outer space in any other manner." The treaty permits placing in orbit weapons other than nuclear weapons and other weapons of mass destruction. Also, the treaty contains no prohibition against nuclear weapons transiting outer space, as long as they do not enter into an earth orbit and they do not explode in outer space.

The Outer Space Treaty also prohibits the establishment of military bases, the testing of weapons, and the conduct of military maneuvers on the moon or other celestial bodies. It permits these activities in orbit around the Earth, and in other places in outer space. Similarly, there is no prohibition against establishing military space stations or operating other satellites with offensive or defensive capabilities.

The *Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space and Under Water* (the Limited Test Ban Treaty, 1963) prohibits all nuclear explosions in outer space. Accordingly, a party to this agreement may not lawfully explode a nuclear device in outer space in order to disable an adversary's satellites by means of the electro-magnetic pulse generated by a nuclear explosion, or by its other effects. A nation operating its own satellite systems is unlikely to take such an action in any event, since its own satellites would be subject to the same effects as those belonging to its adversary.

The *Treaty on the Limitation of Anti-Ballistic Missile Systems* (the ABM Treaty, 1972) provides that no party may "develop, test or deploy space-based ABM systems or components."

Under a 1997 theater missile defense (TMD) agreement not yet ratified by the Senate, the United States and Russia have agreed not to place in space theater missile defense interceptor missiles "or space-based components based on other physical principles, whether or not part of a system, that are capable of substituting for such interceptor missiles."

A number of arms control agreements provide that no party will interfere with the others' "national technical means of verification." Translated, this means no interference with the orbiting imaging systems used to monitor the strategic arms of another party.

Read together, these agreements permit the development, testing, and deployment of anti-satellite and satellite-defense systems unless they involve either the stationing or testing of nuclear devices in outer space or the orbiting of systems that also have ABM or ATM capabilities. Their use is subject only to (1) the general principles of international law relating to the use of force; (2) the principle of non-interference with the space systems of other nations in peacetime, subject to the right to use force in self-defense and when authorized by the UN Security Council; (3) the law of war during international armed conflicts; and (4) obligations under relevant arms-control agreements not to interfere with other parties' national technical means of verification. This leaves a very broad range of permissible "space-control" systems and operations.

In a non-nuclear conflict, the parties might very well determine that the treaty prohibitions against placing nuclear weapons in orbit, against exploding nuclear devices in outer space, and against placing ABM components and ATM interceptors in orbit remain consistent with a state of limited armed conflict. Those obligations may well serve to avoid escalation of the conflict to the nuclear level. The parties' conclusions as to the obligation not to interfere with other parties' national technical means of verification will probably depend to a great extent on the circumstances of the conflict.

D. Domestic Law and Policy.

A federal statute, 18 USC 1367, makes it a felony to intentionally or maliciously interfere with a communications or weather satellite, or to obstruct or hinder any satellite transmission. The application of this statute to national security information operations is discussed in the companion assessment of domestic legal issues.

U.S. domestic policy on developing space control capabilities has been inconsistent at best. By the early 1980s the U.S. Air Force had developed an anti-satellite missile with an explosive warhead that was carried aloft by an F-15 fighter and launched at high altitude. A test of this system was conducted in 1985 against a U.S. satellite whose useful life had expired. Congress soon thereafter decreed that no appropriated funds were to be used to test any weapon against an object in orbit. In 1987 the USAF program was terminated. At the time, it appeared that members of Congress voting for the ban had done so for a variety of reasons, among which were: (1) support for the broad principle that space should be free from human conflict; (2) dismay that the first test had generated 285 pieces of trackable space debris; (3) concern that further testing of an anti-satellite capability might interfere with continuing strategic arms control negotiations; and (4) concern that the United States should not press ahead with testing an anti-satellite system when the nation had yet to decide where its own long-term interests lie. Concerning this last point, it was obvious that there is a military interest in being able to defend your own space systems and having the ability to interfere with your adversary's, but there was also a contrary consideration that the long-term interests of the United States – as the nation that depends most heavily on space systems – may be better served by promoting the development of a regime of international law that prohibits any interference by one nation with the space systems of another, and inhibits the acquisition of the capability to do so. That fundamental debate has yet to be pursued to a definitive conclusion.

Later, when public attention was drawn to the possible use of lasers as anti-satellite weapons, Congress prohibited the use of appropriated funds to illuminate any object in orbit with a laser. This restriction was removed in 1995. In October 1997 the U.S. Army conducted a test in which it illuminated an Air Force satellite nearing the end of its useful life with the MIRACL laser, located at White Sands, New Mexico. Despite public announcements that the purpose of the experiment was purely defensive in nature – to observe the effects of the laser on the satellite's optical sensors in order to better protect U.S. satellites from deliberate or accidental laser illumination – a public furor ensued. Shortly thereafter President Clinton exercised his short-lived item veto authority to delete funds from the FY 98 DoD Authorization Act for development of an Army Kinetic Energy Anti-Satellite Missile and two other projects that he considered to be related to space control. Congress approved additional funds for space control projects in the FY 1999 DoD Authorization Act and urged expenditure of the FY 98 funds that were restored after the Supreme Court ruled that the item veto was unconstitutional.

At this point, it seems fair to say that the United States has not arrived at a consensus on the fundamental policy issues concerning space control. It seems likely for the near future that the development of such systems will continue, with renewed controversy to be expected as soon as a decision is imminent on the deployment, or even advanced testing, of an operational system.

E. International Efforts to Control "Weaponization of Space".

Over the last decade there has been strong support in the UN General Assembly for negotiation in the Conference on Disarmament (CD) of a draft treaty banning weapons in space. The most recent action by the General Assembly was its adoption on 4 December 1998 by a vote of 165-0-4 of a resolution entitled "Prevention of an arms race in outer space." This resolution calls for reestablishment by the CD of an Ad Hoc Committee on the Prevention of an Arms Race in Outer Space that existed in prior years. Canada and Egypt are actively promoting consideration of a "no weapons in space" treaty in the CD, but so far they have garnered little active support among the other CD members. Both Russia and China have also announced their support for negotiations to ban "weaponization of space," but neither has advanced a specific proposal with much vigor. In summary, there appears to be widespread lukewarm support for the general idea of a treaty banning an "arms race in space," but the subject enjoys a low priority at the moment and no draft treaty has garnered significant support. This may all change if and when a nation or nations are known to have deployed operational space control systems, or are on the verge of doing so.

Chinese and Russian support for a ban on "weaponization of space" is seen in some quarters as ironic, since China is reported to be developing a ground-based anti-satellite laser system and Russia is the only nation known to have once had an operational anti-satellite missile. There have been a number of reports that the Soviet Union developed a "co-orbital ASAT" that was launched into orbit, where it maneuvered close enough to a target satellite to destroy the target by exploding. Reportedly, the Soviet system was tested against objects in space 20 times and became operational in 1978. Russia consistently denied that it had tested or deployed such a system until September 1997, when press reports indicate that President Yeltsin said in a letter to President Clinton that Russia at one time possessed an anti-satellite capability, but that it had since "renounced" it.

F. Assessment.

There is no legal prohibition against developing and using space control weapons, whether they would be employed in orbit, from an aircraft in flight, or from the Earth's surface. The primary prohibition is against weapons that entail the placing of nuclear weapons in orbit or that would employ a nuclear explosion in outer space. The use of space control systems in peacetime would be subject to both the general principles of international law and to treaty obligations not to interfere with other nations' space systems and national technical means of verification. These obligations would probably be suspended during an international armed conflict, during which the parties' conduct would be governed primarily by the law of war. U.S. domestic policy on space control, however, is at best unsettled.

V. COMMUNICATIONS LAW

A. International Communications Law.

International communications law consists primarily of a number of bilateral and multilateral communications treaties. The most significant of these treaties is the *International Telecommunications Convention of 1982* (ITC), which has over 140 parties and which became effective for the United States in 1986. This agreement, often referred to as the Nairobi Convention, is the latest in a series of widely adhered to multilateral telecommunications conventions signed in this century, which were preceded by multilateral agreements in the late 1800s providing protection for submarine cables. The current series of agreements establishes the International Telecommunication Union (ITU), which has the status of a specialized agency of the United Nations, and they invest the ITU with the authority to formulate telegraph and telephone regulations which become binding legal obligations upon formal acceptance by ITU member nations. These agreements also establish mutual legal obligations among the parties, several of which are directly relevant to information operations.

Perhaps the most significant of these obligations is in Article 35, which provides that all radio "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 or of recognized private operating agencies, which carry on radio service, and which operate in accordance with the provisions of the Radio Regulations." "Harmful interference" is defined in Annex 2 to the Convention as "interference which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations." One of the clearest violations of this provision would be the jamming or "spoofing" of a radio navigation service. Without speculating on all the possible permutations of the application of this provision to the broad range of information operations, suffice it to say that this provision on its face would appear to restrict many such operations that involve the use of radio broadcasting.

On the other hand, Article 38 of the ITC provides a specific exemption for military transmissions: "Members retain their entire freedom with regard to military radio installations of their army, naval and air forces." In July 1994, when the United States was considering broadcasting messages to the Haitian people from U.S. military aircraft in international airspace urging them not to set out to sea in hazardous vessels, the Office of Legal Counsel in the Department of Justice relied on the military exemption in Article 38 as one of several bases for determining that the ITC does not prohibit such activity. Article 38 goes on to say, "Nevertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations." While this provision indicates that military installations do not have carte blanche to interfere with civilian communications, the phrase "so far as possible," read together with the specific exemption for military radio installations, provides considerable room for maneuver for information operations conducted by military forces.

The ITC also provides specific authority for its member nations to interfere with international telecommunications in certain circumstances:

- Article 19 allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or part thereof, except when such notification may appear dangerous to the security of the State."

- Article 19 also permits members to "cut off any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

- Article 20 reserves the right of members "to suspend the international telecommunication service for an indefinite time, either generally or only for certain relations and/or certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Members through the medium of the Secretary-General."

Finally, it seems clear that the ITC's provisions apply primarily in peacetime. The treaty does not specifically state how – if at all – it will apply during an armed conflict. Nevertheless, there is ample precedent in which nations have demonstrated conclusively that they regard the provisions of international communications conventions as being suspended between belligerents engaged in armed conflicts. Prior to the First World War, for example, all the major European nations were parties to the 1884 *Convention for Protection of Submarine Cables*. The first day of the war, the British Navy pulled up and cut the five major submarine cables serving Germany. Throughout all the wars of this century, communications facilities of all sorts have been regarded as priority military targets. Since some of the parties to the ITC and other multilateral communications conventions are likely to be neutrals in armed conflicts between other nations, the result may become somewhat complicated. Most ITC obligations will be considered to be suspended among the belligerents, but they will remain in effect between each belligerent and the neutral parties to the agreement, as well as among the neutral parties.

Note: The issue of the extent to which a neutral nation or an international communications consortium may continue to provide communications services to a belligerent is discussed in the law of war section of this paper.

The United States has not entered into bilateral communications agreements with very many nations, primarily because the ITC and the ITU provide a framework for handling most international communications issues. As one might expect, the need for bilateral communications agreements has arisen for the United States primarily with Canada and Mexico, because of the potential for interference in broadcast communications across our common borders. A number of bilateral communications agreements have also been negotiated between the United States and nations where U.S. military forces are stationed. There is a potential for such bilateral agreements to either restrict or facilitate information operations by U.S. military forces. The agreements concerned should be consulted when such an issue arises.

B. Domestic Communications Law.

The ITC and its predecessors obligate each Member nation to suppress acts by individuals or groups within its territory that interfere with the communications of other members. In partial satisfaction of this obligation, in 1934 Congress enacted 47 USC 502, which provides, "Any person who willfully and knowingly violates any rule, regulation, restriction, or condition . . . made or imposed by any international radio or wire communications treaty or convention, or

regulations annexed thereto, to which the United States is or may hereafter become a party, shall, in addition to any other penalties provided by law, be punished, upon conviction thereof, by a fine of not more than $500 for each and every day during which such offense occurs." In October 1993, when the United States was considering broadcasting radio messages to the people of Haiti supporting the return of democracy in that nation, the Office of Legal Counsel of the Department of Justice issued a written opinion to the effect that 47 USC 502 does not apply to the actions of U.S. military members executing the instructions of the President acting within his constitutional powers to conduct foreign policy and to serve as Commander-in-Chief of U.S. military forces. Further discussion of this statute can be found in the companion assessment of domestic legal issues in information operations.

C. Assessment. International communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime. The established practice of nations provides persuasive evidence that telecommunications treaties are regarded as suspended among belligerents during international armed conflicts. Domestic communications laws do not prohibit properly authorized military information operations. Accordingly, neither international nor domestic communications law presents a significant barrier to information operations by U.S. military forces.

VI. IMPLICATIONS OF OTHER TREATIES

The State Department's most recent published list of international agreements to which the United States is a party, *Treaties in Force*, January 1, 1997, is 485 pages long. The United States is a party to literally thousands of multilateral and bilateral international agreements. From their sheer numbers, one would think it inescapable that lurking somewhere in those agreements are provisions that will affect particular information operations activities. This section attempts only to highlight certain kinds of "typical" agreements that are likely to contain obligations relevant to the conduct of information operations.

A. Mutual Legal Assistance Agreements. Mutual legal assistance agreements (sometimes called judicial assistance agreements) obligate each party to gather and provide evidence located in its territory concerning litigation or criminal prosecutions that occur within the jurisdiction of another party requesting such assistance. The United States is a party to several dozen mutual legal assistance agreements. Some of these agreements apply only to the management of particular litigation or to certain types of offenses such as drug trafficking and money laundering. Only a few mutual legal assistance agreements apply broadly to all law enforcement investigations and prosecutions. Such an agreement may supply the only domestic legal authority for the assisting party to investigate offenses that did not occur within its jurisdiction, and it also establishes procedures that expedite the requested assistance. To be effective in helping to suppress computer crimes and other high-tech offenses, mutual legal assistance agreements must either expressly cover such offenses or they must apply broadly to all crimes.

B. Extradition Agreements. Extradition agreements obligate the parties in certain circumstances to deliver persons accused of crime to the other party for criminal prosecution. The United States is a party to more than a hundred bilateral extradition treaties, as well as to a 1933 Convention on Extradition to which thirteen nations in the Americas are parties. If no extradition treaty is in effect, a national government often will have neither an international obligation nor the domestic authority to deliver custody of an individual to another nation for the purpose of prosecution. It is important that the list of offenses covered by such agreements include computer intrusions and other high-tech crimes. In addition, the effectiveness of extradition treaties is often frustrated by provisions providing that the requested nation will not extradite its own citizens, or that it will not extradite persons who commit crimes for political reasons.

NOTE: The Department of Justice has undertaken a major initiative with the "G8" countries (the other seven being the United Kingdom, Germany, Japan, Italy, Canada, France, and Russia) to modernize the domestic criminal law of each nation to adequately provide for the investigation and prosecution of computer intrusions and other high-tech crimes, and to put into place any needed improvements to international agreements providing for mutual legal assistance and extradition. In December 1997 the Attorney General hosted a meeting of the G8 Justice and Interior Ministers to discuss these issues, and a number of follow-up working group meetings have been held since that time. The United States has also participated in a project undertaken by the Council of Europe to draft an international convention on "cyber-crime." Recently the United States undertook similar efforts in the Organization of American States and at the United Nations.

C. The United Nations Convention on the Law of the Sea (UNCLOS). Many provisions of this treaty, which is before the Senate for advice and consent, are considered to express customary international law. Some of the provisions discussed here are among them, and are therefore considered to be binding on all nations whether or not they are parties to the Convention. Others constitute new obligations. One principle widely accepted as existing customary international

law is the obligation in Article 19 for a vessel exercising the right of innocent passage through a nation's territorial sea not to engage in activities "prejudicial to the peace, good order, or security of the coastal State." The prejudicial activities listed in Article 19 include:

> "- any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations
> - any act aimed at collecting information to the prejudice of the defence or security of the coastal State
> - any act of propaganda aimed at affecting the defence or security of the coastal State
> - any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State"

Once UNCLOS is in general effect, these restrictions on activities aboard vessels in a coastal state's territorial sea will be of relatively minor importance because UNCLOS limits the width of the territorial sea a nation can claim to twelve nautical miles. At present, a number of nations claim territorial seas as wide as 200 miles. The twelve-mile limitation on the width of the territorial sea, together with other important guarantees UNCLOS establishes for the free operation of military aircraft and vessels, have led DoD to strongly support ratification of UNCLOS.

Article 109 of UNCLOS provides that all "States shall co-operate in the suppression of unauthorized broadcasting from the high seas" and defines unauthorized broadcasting, for the purposes of the Convention, as "the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to international regulations." The international regulations referred to consist primarily of the provisions of the Nairobi Convention and the ITU's Radio Regulations discussed in section V of this paper. This provision, which is generally regarded as establishing new law, was designed to deal with "pirate radio" broadcasting from vessels and platforms on the high seas, which became a significant problem for a number of countries in the 1960s. These broadcasts were primarily commercial in nature; by operating from the high seas they escaped the coastal state's regulation and taxation. Article 109 confers jurisdiction to prosecute persons engaged in pirate radio broadcasts upon the state whose flag the ship flies, the state where a broadcasting installation is registered, the state of which the broadcasting person is a citizen, any state where the transmissions can be received, and any state where authorized radio communication is suffering interference. Article 109 also provides that any state having jurisdiction to prosecute may "arrest any person or ship engaged in unauthorized broadcasting and seize the broadcasting apparatus."

Article 113 requires parties to adopt domestic criminal legislation punishing willful or culpably negligent damage to submarine cables belonging to other parties by ships or persons under their jurisdiction.

These UNCLOS provisions have the potential to affect only a narrow category of information operations, but they will have to be considered when decisions are made concerning those operations to which they do apply, at least in peacetime. UNCLOS does not expressly address how it will apply during an international armed conflict. In accordance with the general principles discussed in the introduction to this paper, provisions determined to be incompatible with a state of armed conflict will be regarded as suspended among the belligerents. The established practice of nations leaves no doubt that Article 19's regime governing innocent passage through the territorial sea will be suspended between belligerents. The same can be said with a high degree of confidence concerning Article 113's protections for submarine cables.

Article 109's provisions for the suppression of unauthorized radio broadcasting from the high seas are relatively new, with little established practice. Analytically, there would seem to be little reason to suspend its application to commercial broadcasters during an armed conflict, but it would almost certainly not apply to broadcasts from the high seas conducted by a belligerent for military or diplomatic purposes.

D. Treaties on Civil Aviation. The United States is a party to a number of treaties concerning civil aviation, the most significant of which is the 1944 *Convention on International Civil Aviation*. This treaty, which has more than 180 parties, is often referred to as the Chicago Convention. It establishes the International Civil Aviation Organization (ICAO) and provides the basic legal framework for international civil aviation. The Convention does not directly apply to state aircraft, except for the obligation stated in Article 3(d): "The contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard for the safety of navigation of civil aircraft." This concern for safe navigation by civil aircraft is also reflected in Article 28, which provides that each party will provide navigation and communications services as agreed upon through ICAO procedures, and in Article 37, which provides that the parties will comply with "international standards and recommended practices and procedures" on a variety of subjects including communications systems and air navigation aids. Over the years the ICAO Council has developed and adopted 18 technical Annexes to the Chicago Convention. Annex 10, Aeronautical Telecommunications, contains agreed provisions on aeronautical communications, navigation and surveillance. While military aircraft are not directly bound by these provisions, their obligation of "due regard" for the safety of civil aircraft generally includes an obligation not to interfere with these systems.

The United States is currently engaged in negotiations in ICAO concerning the role to be played by the Global Positioning System in future navigation systems for international civil aviation. In particular, an accommodation must be reached between ICAO's interest in ensuring that navigation services essential to the safety of international civil aviation are not interrupted during an armed conflict, and the military imperative for the United States to be able to deny the use of GPS to a military adversary. Similar issues are certain to arise in the future in which information operations activities may create implications for the safety of international civil aviation.

The Chicago Convention is rare among multilateral treaties in that it has a specific provision concerning its application during armed conflict. Article 89 provides, "In case of war, the provisions of this Convention shall not affect the freedom of action of any of the contracting States affected, whether as belligerents or as neutrals. The same principle shall apply in the case of any contracting State which declares a state of national emergency and notifies the fact to the Council." Upon reflection, however, this provision is unlikely be applied as broadly as its language indicates. It seems clear that many provisions of the Convention are inconsistent with a state of armed conflict. The most obvious is the principle that aircraft not engaged in scheduled airline service have the right to free passage into or through the airspace of other parties. Other provisions do not appear to be incompatible with a state of armed conflict among some of the parties. For example, the existence of a state of armed conflict among certain parties should not be regarded as suspending the belligerents' obligation to carry out their combatant activities with due regard for the safety of civil aviation. Accordingly, Article 89 does not provide much help in deciding what provisions of the Convention will remain applicable during an armed conflict, and resort will still be required to the general principle that only those obligations that are incompatible with a state of armed conflict will be suspended, and only among the belligerents.

E. Treaties on Diplomatic Relations. The United States is a party to the 1961 *Vienna Convention on Diplomatic Relations*, a widely adhered to treaty establishing obligations among its parties concerning the treatment of diplomatic personnel and premises. Among the protections afforded a party's diplomatic mission in the territory of another state are the right to inviolability of the premises of the mission (Article 2); its "archives and documents" (Article 24); the private residences, papers, correspondence, and property of diplomatic agents (Article 30); and diplomatic communications (Article 27). The treaty further provides that the mission may communicate with its government and other missions and consulates of its government by "all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State." Conversely, the treaty imposes certain duties on diplomatic missions. Article 41 provides that personnel of the mission must respect the laws and regulations of the receiving state, that they must not interfere in the receiving state's internal affairs, and that the "premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State." Article 45 provides that the duties of the receiving state continue in force even in the case of armed conflict between the parties, or if diplomatic relations are broken off between them, even though the staff of the mission is recalled. Planning for any information operations activity that involves diplomatic premises, persons, archives, documents, or communications, either as an instrument or as a target of the operation, must take into account these international legal obligations.

F. Treaties of Friendship, Commerce, and Navigation. The United States is a party to a large number of bilateral agreements with other nations providing reciprocal arrangements for expedited tourism, trade, and transportation between the parties. These agreements have various titles, and their provisions differ somewhat. Most such agreements do not contain specific provisions on telecommunications, and they constitute perhaps the archetype of agreements that are likely to be regarded as suspended during an armed conflict because their provisions expediting free travel and trade between the parties are incompatible with hostilities between them. Nevertheless, planning for information operations, especially in peacetime, should include a review of all significant international agreements between the United States and any other nation that may be affected.

G. Status of Forces and Stationing Agreements. When the military forces of one nation are present in the territory of another nation with its consent, it is customary for the nations involved to execute written agreements establishing the rights and obligations of the parties concerning the visiting forces. "Stationing agreements" establish the consent of the host nation to the presence of foreign troops; set agreed limits on their numbers, equipment, and activities; and identify facilities for their use. These topics may also be dealt with in a "defense cooperation agreement" or some other agreement providing for the overall defense relationship between the parties. It is also common for the parties to execute a "status of forces" agreement (SOFA) that addresses the allocation of various kinds of legal jurisdiction over the visiting forces. The best known of these agreements is the 1951 *Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces* (NATO SOFA). As of the end of 1998 the United States was a party to 103 SOFAs, most of which follow the general pattern of the NATO SOFA. SOFAs are necessary because of an overlap of legal jurisdiction exercised by the sending and receiving states. The receiving state has jurisdiction over persons and activities in its territory, while the sending state has both the right and the duty to exercise control over its armed forces, which is clearly a core sovereign function.

Since the full concurrent exercise of the normal jurisdiction of the sending and receiving states is impractical, status of forces agreements allocate criminal and civil court jurisdiction between the sending and receiving states, and also exempt the visiting force and its members from certain taxes, customs fees and procedures, immigration formalities, and most host nation licensing and inspection requirements. Typically, an administrative claims procedure is established for personal injuries and property damage caused by the visiting force. Another common provision requires that the visiting force and its members "respect" the host nation's laws. (This requirement will be discussed in detail in the next section of this paper). The NATO SOFA is implemented in most NATO countries by separate, more detailed, bilateral supplementary agreements, and by numerous other bilateral agreements on specific subjects including communications.

These agreements contain provisions that must be taken into account if U.S. military forces intend to engage in information operations activities while present in the territory of the receiving state.

- For example, many such agreements require that the United States notify the host nation of any significant change in the capabilities or uses of installations made available for the use of U.S. military forces. If U.S. authorities intend to conduct information operations activities from such installations, a determination must be made as to whether the relevant agreements require notifying the host nation, and perhaps even requesting its consent.

- Stationing agreements often provide that the visiting U.S. forces may install and use various communications equipment, but they often provide as well that such equipment must not interfere with host nation communications systems and that it must be used in accordance with host nation laws and regulations. If this equipment is to be used for information operations activities, it must be determined whether the contemplated activities are consistent with these obligations.

- Many stationing agreements authorize or even obligate the visiting force to use the receiving state's military and civilian communications systems. Commonly, there are obligations that any U.S. use of host nation communications systems must not cause interference and that such use must be in accordance with host nation laws and regulations. The potential for information operations to cause interference with the host nation's communications system and the possible application of host nation laws and regulations must be carefully considered, along with the fact that the conduct of offensive information operations through host nation communications systems may subject them to possible countermeasures and acts of self-defense in peacetime, and may make them legitimate military targets during an armed conflict.

Finally, if a host nation discovers that its territory and facilities have been used without its knowledge as a base for U.S. information operations of a nature that may tend to involve it against its will in a conflict or dispute, U.S. diplomatic and military relationships with the host nation are likely to suffer. The host nation could well take the view that in principle there is little difference between using an ally's territory to launch air strikes and using it to launch computer network attacks or other information operations activities. As a practical matter, computer network attacks are much more difficult to identify, trace, and attribute. However, it will not always be impossible to do so, particularly when information on such attacks is available from intelligence sources. Accordingly, decisions concerning whether to conduct information operations from the territory of an ally, and especially whether to do so without the host nation's knowledge and consent, must be made at senior policy levels.

VII. FOREIGN DOMESTIC LAWS

A. Introduction. Laws enacted by other nations may have important implications for information operations activities conducted by U.S. military forces. As discussed in the companion assessment of domestic legal issues in information operations, U.S. criminal statutes addressing computer-related offenses, space activities, communications, and the protection of classified information all raise important issues for information operations. These U.S. statutes are part of the federal criminal code. Similarly, foreign laws affecting U.S. information operations activities will most likely also consist of criminal statutes.

The sophistication of foreign domestic law on high-tech activities varies enormously, and it will continue to do so for the foreseeable future. The more technologically advanced countries tend to be better aware of the dangers created by computer hackers and other high-tech criminals, so they typically take the lead in putting legislation into place to criminalize such behavior. It is no accident that the Justice Department's international program to promote appropriate changes to mutual legal assistance treaties and other nations' domestic laws, which was discussed in Section VI of this paper, concentrated first on the G8 countries and the Council of Europe. There are other important variables at work besides technological advancement, however, including each nation's public opinion and policy positions concerning high-tech offenses, especially computer hacking. There are persons in every country, including the United States, who regard hackers as essentially harmless pranksters. There is a well-established minority view that the Internet and all the computer systems connected to it should be free game, and that defeating attempts to gain unrestricted access to these resources or imposing regulations on personal conduct on the Internet are repressive violations of the hackers' civil liberties. The argument is even advanced that hackers provide valuable assistance to the operators of the computer systems they attack, by revealing vulnerabilities that otherwise might have been exploited by sinister persons with malicious motives. On the international scene, there is the additional factor that many individuals love to see one of their fellow citizens succeed in pulling the tail of richer and more powerful nations, especially the United States.

As a result, the state of domestic laws dealing with high-tech misconduct varies enormously from country to country. This has important implications for U.S. information operations for two basic reasons: (1) The state of a nation's domestic criminal law directly impacts the assistance that the nation's public officials can provide in suppressing certain behavior by persons operating in its territory; and (2) The state of the nation's domestic criminal law may have a significant effect on U.S. information operations conducted in the nation's territory or involving communications routed through the nation's communications systems.

B. Cooperation in Investigations and Prosecutions. It should be readily apparent that law enforcement officials cannot prosecute an individual for conduct that is not defined as a crime in the applicable criminal law. It may be less obvious, but equally important, that in most constitutional governments law enforcement officials may not use their authority to conduct criminal investigations unless the alleged conduct constitutes a crime. If a hacker in Country X uses the Internet to gain access to a DoD computer in the Pentagon, copies sensitive data, deletes or corrupts data, and installs malicious logic, the law enforcement officials of Country X may be able to assist in investigating that conduct and may be able to extradite the offender to the United States only if one or more of the hacker's actions constitute a crime under that nation's law. Even where such legislation exists, the legal system may still not be able to provide either extradition or meaningful criminal punishment, as occurred in the case of a young Israeli hacker given a

suspended sentence by an Israeli court after he participated in a series of unlawful intrusions into DoD computer systems in early 1998.

The domestic laws of some nations may also permit the use of devices specifically designed to frustrate attempts to trace Internet communications to their source. Since geography is essentially irrelevant to communications on the Internet, devices such as anonymous remailers, which strip off all information about the originator of a message, make it possible for a hacker located anywhere – even in the United States or other country – to avoid identification by routing his or her message through the anonymous remailer. In this way, weaknesses in the domestic law of one state may provide impunity to hackers everywhere. The weakest link therefore threatens law enforcement even in countries with robust and sophisticated laws. Accordingly, the imperative to bring domestic laws in every nation up to a reasonable standard should be readily apparent.

C. Effect of Foreign Domestic Law on Actions of U.S. Information Operators. If a CINC or a JTF commander decides to order execution of a certain information operations activity by forces under his or her command who are deployed in a foreign country, the commander may have to consider whether or not such activity is prohibited under local law. The answer may be important at two different levels of analysis: (1) The individuals who issue or execute such an order might be subject to prosecution in a host nation criminal court; and (2) The commander might feel obligated on a policy basis to refrain from issuing such an order.

If a U.S. military member issued an order or performed an act in the course of his or her official duties overseas that was a crime under host nation law, the member could very well be subject to prosecution in a host nation criminal court. Under many SOFAs, an act done in the course of a military member's official duties falls within the primary right to exercise jurisdiction of the sending state, but that rule applies only when the conduct constitutes an offense under the law of both nations, or only under U.S. law. Where the conduct alleged constitutes an offense only under the law of the host nation, the host nation has exclusive jurisdiction to prosecute. The United States has consistently taken the position that it would be intolerable for a U.S. military member to be criminally prosecuted for performing an act that is legal under applicable U.S. law, such as the Uniform Code of Military Justice (UCMJ), and which he or she was instructed to perform in the execution of an official duty. A similar issue arose recently in connection with the adoption by several NATO member nations of domestic laws making it a crime to possess anti-personnel land mines (APLs). There is no similar crime under the UCMJ. In several cases, the nations concerned have agreed to permit the U.S. forces to retain their APL stockpiles in the host nation's territory for at least some period of time. In these cases, either specific exemptions from the host nation law or agreed screening procedures for prosecutions have had to be devised to prevent prosecutions of U.S. military members for performing their official duties.

A similar problem would arise in information operations if a host nation criminal law applied which had no counterpart under the UCMJ. Such a situation may be much more likely to occur than it would seem at first glance. If the host country has a reasonably sophisticated computer crimes law, it will probably cover a number of acts that may be performed as information operations activities, including using a computer to obtain unauthorized access to another computer, electronic communications, or data in storage; or to transmit malicious logic; or to interfere with a satellite or with the licensed radio communications of another party to the Nairobi Convention. All these acts would appear to violate U.S. domestic statutes, but a U.S. military member will not be instructed to perform them unless a specific statutory exemption exists or the statute in question has been authoritatively interpreted as not applying to his or her actions. (See the discussion of issues of statutory interpretation in the companion assessment of U.S. domestic

legal issues in information operations.) Accordingly, the host nation would have exclusive jurisdiction to prosecute. The lesson we need to extract from this discussion is that as we busily encourage other national governments to enact effective legislation on high-tech crime, we need to ensure that such legislation provides an effective exemption for U.S. military forces who may be stationed in that country and who may be engaged in information operations.

In practice, such prosecutions are most unlikely because if U.S. military authorities become aware that performance of certain information operations within the territory of a specific host nation, or that produce harmful effects within its territory, will subject military personnel to possible host nation criminal prosecution, those U.S. military authorities are most unlikely to order that such operations be conducted. The result will be that U.S. forces are unable to conduct certain activities they would otherwise conduct, or perhaps that they will have to use forces elsewhere to conduct the operation. The issue thus becomes not so much one of the prospect of criminal prosecution of individual servicemembers but rather of a limitation on the conduct of U.S. information operations.

This consideration may be not only a policy issue – it may involve binding legal obligations under a status of forces or similar agreement. For example, Article II of the NATO SOFA provides, "It is the duty of a force and its civilian component and the members thereof as well as their dependents to respect the law of the receiving State . . . ." Similar language appears in most other SOFAs to which the United States is a party. Considerable practice has accumulated concerning the application of this obligation to "respect" the law of the receiving state. It has often been argued that the drafters could have said the visiting force must "comply" with host nation law but instead chose the less definite term "respect." The product of almost fifty years of U.S. practice in implementing SOFAs worldwide appears to be that U.S. visiting forces will generally observe the content of host nation law, but are exempt from the law's procedural requirements such as licensing, inspection, and reporting. If U.S. visiting forces seek to avoid the application of the substance of a foreign law, they generally request the host nation to grant them a specific exemption or at least to reach an understanding that a particular host nation law will not be enforced against the visiting forces.

If a contemplated information operation activity appear to conflict with host nation law, the commander concerned might choose to consult with host nation officials in an effort to resolve the issue. If time or other circumstances do not permit such consultations, the commander should carefully consider whether the activities in question should be conducted by forces outside the territory of the host nation concerned, and in a manner that would not make use of or affect that nation's communications systems. U.S. military and diplomatic authorities should be able to manage host nation legal issues if we identify them early on and carefully consider the available courses of action.

VIII. IMPLICATIONS OF ESPIONAGE LAW

A brief review of the treatment of espionage under international law may be instructive in predicting how the international community will react to information operations, especially in those mission areas in which the same technical capabilities may be used for both espionage and information operations, and also in other areas where reasonably persuasive analogies present themselves.

A. Espionage under International Law. For our present purposes, espionage may be defined as the covert collection of intelligence about other nations. Espionage is a much narrower topic than "intelligence," much of which is collected via open source information, voluntary exchanges of information among nations, and technical means such as satellite imagery and signals intelligence that are generally accepted as legal by the international community. Roughly stated, covert methods of collecting intelligence are in most cases designed to go undetected by their target, and if detected they are designed to be unattributable to the sponsoring state. Nevertheless, discovery, attribution, and public disclosure occur fairly often.

B. Espionage during Armed Conflict. The treatment of spies during armed conflict is well established in the law of war. A "spy" is defined in the law of war as any person who, when acting clandestinely or under false pretenses, obtains or endeavors to obtain information in the area controlled by a belligerent, with the intention of communicating it to a hostile party. A spy may be a military member or a civilian, and his or her citizenship is irrelevant. Military personnel wearing their own uniforms are not considered to be spies, even if they engage in collecting intelligence behind enemy lines. Only a person gathering intelligence while relying on protected civilian status or while wearing an enemy uniform is considered to be a spy under the law of war. Accordingly, information operations during an armed conflict will not raise any issue of spying under the law of war unless they involve the presence of individuals inside enemy-controlled territory who (1) are engaged in collecting information with the intent of communicating it to a hostile party, and (2) are wearing civilian clothing or enemy uniforms. It seems highly unlikely that the notions of "electronic presence" or "virtual presence" will ever find their way into the law of war concept of spying, for two reasons: (1) If an individual is not physically behind enemy lines he or she is not subject to capture during the mission; and (2) There will be no issue of acting under false pretenses by abusing protected civilian status or by wearing the enemy's uniform. This will exclude most information operations activities from being considered espionage in wartime. Nevertheless, behind-the-lines missions to collect information, or to install devices that enable the collection of information, may well raise wartime spying issues.

If caught in enemy territory, a spy can be punished, after an appropriate trial, under the domestic law of the captor. The punishment can include the death penalty. The nation on whose behalf the spy was acting, however, will not be considered to have violated any international legal obligation. In addition, if individuals who may have engaged in espionage but successfully complete their missions (that is, they have returned to friendly lines) and subsequently are captured while not engaged in acts of spying, they may not be punished for their previous acts of espionage.

C. Espionage in Peacetime. Unlike the relatively well developed treatment of espionage under the law of war, there is very little authority on the treatment of espionage under international law in peacetime. There have of course been many domestic criminal trials of peacetime spies in many countries, including the United States. By contrast, there has been almost no activity

concerning peacetime espionage within the international legal system except for public complaints and the expulsion of implicated diplomats. This may be because the primary harm done to the victim nation consists of the fact that certain secret information has been compromised, which is a more abstract and indirect type of injury than dead or injured citizens, property damage, or invasions of territory. The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called "*tu quoque*" (roughly, a nation has no standing to complain about a practice in which it itself engages). Whatever the reasons, the international legal system generally imposes no sanctions upon nations for acts of espionage except for the political costs of public denunciation, which don't seem very onerous.

The consequences for individuals caught spying, however, can be very serious. Such individuals can be tried for whatever crimes their conduct may constitute under the victim nation's domestic law, whether charged as espionage, as unlawful entry into its territory, or as a common crime such as burglary, murder, theft, bribery, obtaining unauthorized access to state secrets, or unauthorized computer intrusions. This fact accounts to some extent for the widespread practice of assigning intelligence operatives to embassy staff positions in which they enjoy diplomatic immunity from prosecution. The only remedy for an offended host nation is to declare such persons to be *persona non grata*, which obligates the sending nation to remove them from the country.

The treatment of espionage under international law may help us make an educated guess as to how the international community will react to information operations activities. As discussed in Section III of this paper on the use of force, international reaction is likely to depend on the practical consequences of the activity. If lives are lost and property is destroyed as a direct consequence, the activity may very well be treated as a use of force. If the activity results only in a breach of the perceived reliability of an information system, it seems unlikely that the world community will be much exercised. In short, information operations activities are likely to be regarded much as is espionage – not a major issue unless significant practical consequences can be demonstrated.

That leaves the issue of the possible criminal liability of an information operator who may later come into the custody of a nation that has been the victim of an operation in which he or she has engaged. As with a spy, there is no evident theoretical reason why such an individual could not be prosecuted for violation of the victim nation's criminal laws. As a practical matter, however, the problems of detection and attribution of information operations activities at the national level are daunting; the likelihood of being able to prove in court that an individual engaged in a certain information operations activity – while not impossible – seems unlikely. Perhaps the best policy would be to advise information operators not to vacation in locales where the effects of their activities have been felt, at least until a decent interval has passed.

Finally, it deserves mention that there is an established division of labor within the U.S. government between the intelligence community and the uniformed military forces concerning "covert action." Generally speaking, the intelligence community conducts covert action operations in peacetime that do not consist of traditional military activities. It remains to be seen how information operations activities will fall within this division of labor, especially when they are associated with military operations other than war.

D. Assessment. Information operations activities are unlikely to fall within the definition of spying in wartime, although a limited category of activities related to information operations may so qualify. Information operations activities are more likely to fall within the category of

peacetime espionage. Perhaps more importantly, the reaction of the world community to information operations that do not generate widespread dramatic consequences is likely to be very similar to its reaction to espionage, which has traditionally been tepid.

IX. INTERNATIONAL EFFORTS TO RESTRICT "INFORMATION WARFARE"

As soon as the concept of "information warfare" began to receive broad press coverage, discussion began of negotiating a treaty that would prohibit or restrict it. A draft treaty text that circulated on the Internet in 1995 said simply, "The Parties to this Convention agree not to engage in information warfare against each other." The first public governmental initiative was a resolution tabled by Russia in the UN's First Committee in October 1998 that apparently reflected a serious effort to get the UN to focus on the subject. The Russian resolution included a call for states to report their views regarding the "advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons." The United States has taken the position that it is premature at this point to discuss negotiating an international agreement on information warfare, and that the energies of the international community would be better spent on topics of immediate concern such as helping each other to secure information systems against criminals and terrorists. So far there has been little support expressed for the Russian initiative.

There are both similarities and differences between the concept of a treaty to ban or restrict information warfare and similar efforts to prohibit "weaponization of space." One similarity is the political reality that nations lacking a significant new military capability that they perceive will be dominated by a few wealthy and powerful states have a strong incentive to agree to ban or restrict that capability. There may be an even greater incentive to prevent interference with information systems, which all nations possess to some degree, than with space systems, in which only 30 nations are currently active and which are dominated by the United States, Russia, and the European Space Agency. On the other hand, the number of nations that have any reasonable expectation of developing their own space control systems anytime soon can be counted on the fingers of one hand, while anyone with a desk-top computer and an Internet connection thereby has access both to hacker tools and to a wide variety of important information targets worldwide. Accordingly, as nations appraise where their long-term national interests lie, the calculus is quite different as between international legal restriction of the "weaponization of space" and similar control of information warfare. With space systems, most states do not expect to be either an attacker or a defender in the near future. With information systems, all states can reasonably expect to be both.

As with space control, the United States has not yet addressed fundamental policy decisions about where its long-term interests lie in connection with the possible international legal restriction of information operations. On the one hand, there is an obvious military interest in being able to interfere with an adversary's information systems, and in being able to protect one's own. Used as a tool of military power, information operations capabilities have the significant advantage that they minimize both collateral damage and friendly losses of personnel and equipment. Their use may avoid unwanted escalation of a dispute or conflict. They are relatively cheap and require much less in the way of forward basing, deployment, and logistical support than do traditional weapons and their delivery platforms.

On the other hand, as the nation that relies most heavily on advanced information systems, the United States has the greatest vulnerability to attack. This concern would seem to drive U.S. policymakers to consider the merits of international restrictions on information operations. If we could negotiate an effective international ban on certain types of information operations activities, might signing such a treaty best serve our long-term national interests?

The subject of information operations is of course much more complex than that of space control, since there are so many more information systems subject to attack, so many more ways

of attacking them, so many more potential players, plus constant rapid changes in the relevant systems and technologies. As we have learned in our internal U.S. policy deliberations, there are great difficulties in even agreeing on definitions of what ought to be included in discussions of "information warfare" and "information operations." In these circumstances, it seems unlikely that there will be much enthusiasm anytime soon for negotiating an international agreement that would significantly restrict information operations.

X. OBSERVATIONS

There seems to be little likelihood that the international legal system will soon generate a coherent body of "information operations" law. The most useful approach to the international legal issues raised by information operations activities will continue to be to break out the separate elements and circumstances of particular planned activities and then to make an informed judgment as to how existing international legal principles are likely to apply to them. In some areas, such as the law of war, existing legal principles can be applied with considerable confidence. In other areas, such the application of use of force principles to adopting an "active defense," it is much less clear where the international community will come out, and the result will probably depend much more on the perceived equities of the situations in which the issues first arise in practice. The growth of international law in these areas will be greatly influenced by what decision-makers say and do at those critical moments.

There seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations. The principal exception is international criminal cooperation, where current U.S. efforts to improve mutual legal assistance and extradition agreements should continue to receive strong emphasis. Another idea that might prove fruitful is to negotiate a treaty to suppress "information terrorism," but there seems to be little concept at present how such an agreement would operate or how it would reliably contribute value to information assurance and critical infrastructure protection.

There are no "show-stoppers" in international law for information operations as now contemplated in the Department of Defense. There are, however, many areas where legal uncertainties create significant risks, most of which can be considerably reduced by prudent planning. Since so many of these potential issues are relatively novel, and since the actions taken and public positions announced by nations will strongly influence the development of international law in this area, the involvement of high-level policy officials in planning and executing information operations is much more important at present than is the case with more traditional military activities.

IATAC

August 21, 2001

To: Mr. Lawrence Downing/Ms. Zena Rogers
DTIC/OCQ

From: Abraham Usher AU
IATAC Collections Specialist

Re: ADB257057 and ADB257113

This has reference to two documents:

ADB257057 An Assessment of International Legal Issues in Information Operations

and

ADB257113 White House Document Analysis

The distribution statement on both of these documents should be changed to Distribution A – *Approved for public release.*

Thank you,

Abraham Usher

3190 Fairview Park Drive • Falls Church, VA 22042
Phone: 703.289.5454 • FAX: 703.289.5467 • STU-III: 703.289.5462
E-mail: iatac@dtic.mil • URL: http://iac.dtic.mil/iatac • SIPRNET: http://iatac.dtic.smil.mil