International Law Studies - Volume 76
Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell (Editors)

XVIII

"Weapons like to Lightning"[1] US Information Operations and US Treaty Obligations

Jeffrey H. Smith and Gordon N. Lederman

The increasing prevalence of computers in the world economy creates new opportunities for the US to conduct offensive military operations and espionage. However, the US is increasingly vulnerable to computer attack, requiring the United States to defend its military and civilian electronic infrastructure. As a nation committed to the rule of law, the United States must remain within the bounds of international law in the conduct of both offensive and defensive information operations.

This chapter explores the opportunities and restraints offered by international law for the conduct of US information operations. We both summarize and critique the 1999 analysis of these issues by the Office of General Counsel, US Department of Defense (DoD), entitled "An Assessment of International Legal Issues and Information Operations" (hereinafter DoD/GC Paper).[2] The DoD/GC Paper surveys international legal issues ranging from the law of war, to obligations under the United Nations Charter, to a host of treaties signed by the United States. This chapter will explore the impact of US international obligations concerning outer space, international communications, and other issues on the conduct of information operations. It will not

address the law of war[3] or the UN Charter,[4] as they are addressed elsewhere in this "Blue Book."[5]

First, this chapter provides a general overview of the development and conduct of information operations. Second, it briefly outlines the structure of international law, including the existence of treaties and the formation of customary international law. Third, US obligations under international law regarding the use of outer space and the impact of these obligations on the conduct of information operations are examined. Fourth, we will explore treaties and international agreements related to the international communications network and their impact on US information operations. Fifth, a survey of possible treaties and other US obligations under international law is offered as a checklist for military commanders and officials deciding whether to authorize a particular information operation. The chapter concludes by offering some thoughts on the merits of an international treaty concerning information operations. In sum, the international legal obligations analyzed herein complicate US information operations but present no insurmountable barriers to them.[6]

It must also be understood that any information operation may well be taken under the extreme pressure of international conflict, without adequate time to weigh all of the legal and political considerations that ought to be considered. Consequently, careful thought must be given to the host of problems raised by these emerging technologies. Moreover, the rate of change in the information technology world means that the legal and political questions presented may be dramatically altered by new technological developments.

In addition, information warfare presents an interplay between domestic and international law not previously seen. For example, the authority of the United States to detect, track, and respond to an information operation is driven as much by the law governing electronic surveillance of US citizens as by international law governing the use of force. Similarly, the questions of what legal authority authorizes an agency to act—and which agency—are very difficult questions. Although beyond the scope of this chapter, these questions must also be answered well in advance of an international crisis.

Finally, it may be difficult to determine whether an information operation is a hostile attack or a criminal act. This ambiguity raises a multitude of questions about how the US should respond to such an event. Furthermore, a response from the US may have unintended consequences, as decision-makers may not be able to predict the collateral damage that may result. An information operation against one nation's infrastructure may have collateral damage, such as destroying bank records, that is much more severe than was intended. Given the interconnectivity of the Internet, a US information operation may blowback

into the United States. Such a possibility raises several questions concerning the privacy and rights of US citizens.

In sum, information operations present many complex legal and operational issues. To first address them in the heat of an information operation is to risk answering them inappropriately.

The Emergence of Information Operations as a Weapon in the Arsenal of Democracy and as a Threat to Democracy Itself

The benefits of increased efficiency and greater speed brought by the infusion of computer technology—particularly the Internet—into the modern economy come at the price of increased vulnerability to disruption and economic ruin as the result of a computer attack.[7] The United States, as the world's most technologically advanced nation, is best situated to develop mechanisms that import information technology into weapons systems[8] and to exploit other countries' reliance on information technology. Simultaneously, however, the United States itself is vulnerable to economic paralysis resulting from the crippling of key US information technology systems. Indeed, as the Federal Bureau of Investigations' former information technology security director, Jim Settle, has stated, the United States could be brought to its knees within 90 days by 10 hackers.[9] Information warfare could eventually usurp the position of biological and chemical weapons as "the poor man's nuclear weapon" because, like biological and chemical weapons, information warfare does not require sizeable financial investment but, unlike biological and chemical weapons, is potentially easier to use—all that is needed for information warfare is a computer and a modem.

As with any concept of sudden importance, the terms and definitions of information warfare have yet to coalesce into an established lexicon. The most succinct definition of information warfare is offered by Winn Schwartau: "Information warfare is an electronic conflict in which information is a strategic asset worthy of conquest or destruction."[10] The US military uses the term "information operations," which involves "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[11] The term "information systems" refers to "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[12] "Information operations" thus refers to attacks against such infrastructure, organization, personnel, etc.

The military also uses the term "computer network attack," defined as "operations to disrupt, deny, degrade, or destroy information resident in computers

and computer networks or the computers in computer networks themselves."[13] Information operations include a whole host of weapons, including Electro Magnetic Pulse (EMP) and directed energy weapons (such as lasers and high-energy radio frequency guns).

Bureaucratic barriers may have obstructed the conduct of US information operations during the Gulf War and the Bosnia operations.[14] However, the United States did conduct information operations in the 1999 NATO air campaign against Serbia. Army General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, confirmed that the US used information warfare against Serbia during the Kosovo campaign when he stated that "you can assume that we in fact employed some of our systems, yes."[15] Yet, the DoD's after-action report on the air war noted that "the conduct of an integrated information operations campaign was delayed by the lack of both advanced planning and strategic guidance defining key objectives."[16] Indeed, the DoD apparently was concerned about the legalities of full-scale information operations against Serbia, as well as the untested nature of the information warfare arsenal; as a result, the information operations were apparently constrained. Also, the relative decentralization of Serbian computer systems limited the potential for success of information operations. US military forces apparently did confuse and disable the Serbian air defense system using information operations, but these attacks originated with electronic jamming aircraft rather than over computer networks from ground-based sources.[17]

The United States, of course, is a prime target of foreign information operations. Lieutenant General William Donahue, the Air Force's Director of Communications and Information, reportedly stated that, during the Kosovo air campaign, hackers from Chinese Internet addresses targeted NATO networks after NATO's accidental bombing of the Chinese Embassy in Belgrade.[18]

Other countries also recognize the growing and critical importance of information operations. For example, the Chinese military reportedly recognizes and hopes to exploit the potential offered by information operations. On November 2, 1999, Major General Chang Chia-Sheng, director of the simulation center under the Chinese Ministry of National Defense, stated at a news conference that China would be able to launch information warfare against Taiwan by 2005.[19] An article entitled "Bringing Internet Warfare Into the Military System is of Equal Significance with Land, Sea, and Air Power," in *Liberation Army Daily*, the official daily newspaper of the People's Liberation Army's General Political Department, reportedly stated that it was likely that another Chinese military branch, a so-called net force, would be needed to conduct information operations. The article was quoted as saying, "Modern High-Tech Warfare

cannot win without the net, nor can it be won on the net. In the future, there must be coordinated land, sea, air, space, electronic and net warfare. . . ."[20] Other news reports indicate that China and Taiwan are particularly involved in a growing arms race regarding information warfare.[21]

Information operations are thus growing in importance for military operations. It is likely that the United States will utilize information operations in future warfare and peace-enforcement operations. Thus, military and civilian decision-makers must understand the opportunities and restraints offered by international obligations on the conduct of such operations.

A Brief Survey of the Process of International Law

Before looking at specific treaties, it is helpful to have an appreciation for how international obligations arise. Two principles of international law are that, first, sovereign States are equal and independent actors in the international system, and, second, States assume legal obligations only by actually agreeing to do so. States may enter into international treaties and agreements binding the signatory parties. There also exists a body of "customary" international law, composed of practices that are so widely followed by the majority of nations that they are considered obligatory for all. For example, the first satellites launched by the Soviet Union and the United States were seen as benign, and nations lacked the technological ability to interfere with satellites; as a result, it became customary international law that objects in orbit were beyond territorial claims of any nation and that outer space was open to all nations. These concepts were later embodied in international treaties concerning outer space, which will be discussed later in this chapter. As a side note, the development of international law concerning outer space contrasts with that concerning aviation, in which nations produced a highly restrictive legal structure creating the concept of air space and rendering illegal the entrance of aircraft into another nation's airspace.[22]

Countries usually cannot unilaterally withdraw from a treaty unless the treaty provides for such an action, and treaties can only be modified by the agreement of the parties. It should be noted that both treaties ratified by the Senate and executive agreements entered into by the President are equally binding on the United States. Also, many treaties are silent on whether they continue to be in force in the event of conflict or hostilities between the signatory parties; this is important for discerning whether the US is bound by a particular treaty's obligations in the event of an outbreak of hostilities and a US desire to conduct information operations.[23]

US Information Operations in Space

International law concerning activities in outer space is critical for information operations because outer space is a vital battleground for information operations. Space-based systems "perform such functions as communications relay, image recollection, missile warning, navigation, weather forecasting, and signals intelligence."[24] As a result, US information operations will be aimed in part against space-based systems. Such attacks could manifest themselves in attacks against ground stations, jamming communications links, or attacking the satellites in space themselves.[25] Furthermore, as apparently occurred during the Kosovo air campaign, satellites can be used to relay transmissions that are part of a US information operation against a ground-based target.

Since the first satellite was launched by the Soviet Union in 1957, States have signed four major multilateral space treaties: (1) the 1967 Outer Space Treaty;[26] (2) the 1968 Rescue and Return Agreement;[27] (3) the 1972 Liability Convention;[28] and (4) the 1975 Registration Convention.[29] The Moon Agreement of 1979 was not signed by the United States and has in fact only been signed by eleven, and ratified by nine, countries.[30] Emerging from these four major space treaties are several principles concerning the use of space: (1) outer space is free for exploration and use by all States and cannot be subject to any claim of sovereignty; (2) activities in space must be done with due regard for the interest of other States; and (3) States that launch objects into space are liable for any damage they cause. As the DoD/GC Paper highlights, the rules on the use of force such as the law of war and the UN Charter are fully applicable in space. The paper also notes that, while space law contains the principle of non-interference with other States' space systems, this provision might be inapplicable during wartime if the treaties themselves do not remain in effect during hostilities.[31]

Although these treaties strictly limit the use of space for military purposes, they do not outlaw all military activities per se. Rather, the Outer Space Treaty mandates that parties shall 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, or station such weapons in outer space in any other manner" (emphasis added).[32] The Outer Space Treaty also prohibits the establishment of military bases and other types of military activities on the moon.[33] The 1972 Anti-Ballistic Missile (ABM) Treaty provides that no party may "develop, test or deploy" space-based ABM systems or components.[34] As the DoD/GC Paper summarizes, the web of international treaties concerning space prohibits the stationing, testing, or exploding of *nuclear* devices in outer space

and the deployment of a space-based anti-ballistic missile capability. However, despite the existence of certain limitations, the paper concludes that there is no legal prohibition on developing and using *non-nuclear* weapons in space, whether deployed in orbit or via flight from the earth's surface.[35] Seemingly, this conclusion appears to open space to information operations.

Still, the DoD/GC Paper does not explore one possible way in which the Outer Space Treaty might ban information operations utilizing satellites. While the Outer Space Treaty prohibits "objects carrying nuclear weapons or any other kinds of weapons of mass destruction . . . or stationing such weapons in outer space, in any other manner,"[36] it is unclear whether information operations fall into the category of weapons of mass destruction. For example, a computer attack against any national computer system of critical importance (e.g., key banking systems, key medical systems, computer systems controlling dams, oil refineries, and other critical infrastructure installations) could wreak "mass destruction" in the sense of widespread loss of life and property.[37] To the extent that a weapon is judged to be a weapon of mass destruction not because it falls within a certain category of what is already accepted as a weapon of mass destruction, namely, chemical, biological, radiological, and nuclear, but rather based on the weapon's effect, information operations could (if used skillfully) exact a fearful toll on both life and property.[38] Of course, even if certain information operations could constitute weapons of mass destruction, it is unclear what constitutes "carrying" or "station[ing]" such weapons on a satellite. If a satellite is used simply to relay data from a computer in the aggressor country to a computer in the victim country, it is unclear whether such a relay of information would be considered "carrying" or "stationing" as defined by the Outer Space Treaty. However, one could imagine a situation in which a particular program for information warfare is stored in a satellite's computer, waiting for the proper signal or timing for delivery to a ground-based target. In this case, the Outer Space Treaty could be interpreted as prohibiting the use of satellites for information warfare.

If the erratic development of US policy on anti-satellite weapons is any indication, policy regarding information operations in space may remain unsettled for many years. For example, in the early 1980s, the Air Force developed an anti-satellite missile designed to be fired from an F-15 fighter flying at a high altitude. After the system was tested in 1985, Congress prohibited the appropriation of funds for anti-satellite weapons to be tested against an object in orbit, leading to the termination of the program in 1987. Congressional critics of the anti-satellite weapons program argued that: (1) outer space should remain free from warfare; (2) tests in space of anti-satellite weapons created space debris; (3) testing of anti-satellite weapons might interfere with arms control negotiations;

and (4) the United States did not necessarily want to encourage other nations to develop an anti-satellite weapon system given its own heavy reliance on satellites. In contrast, supporters of anti-satellite programs argued that the United States should have the ability to attack opposing States' satellites and should invest in defending its own satellites.

By the early 1990s, anti-satellite technology had moved away from missiles and toward lasers. Congress first prohibited and then later allowed the use of appropriated funds for a test of a laser against an orbiting satellite. In October 1997, the US Army tested its MIRACL laser against an aging satellite. While the Army tried to construe the test as purely defensive in nature (namely to observe the effects of a laser on satellites in order to generate information for protecting satellites), a public uproar followed. President Clinton subsequently used his then-existing line-item veto authority to strike funds from the fiscal year (FY) 1998 DoD Authorization Act for projects related to an anti-satellite and space control program. Subsequently, following the Supreme Court's ruling that the line-item veto was unconstitutional, Congress approved funds for anti-satellite weapons in the FY 1999 DoD Authorization Act.[39] Accordingly, it is likely that the increased use of space-based systems as instruments in information warfare will engender criticism from opponents of anti-satellite weapons systems, who will argue that the United States should not further militarize space. However, the assumption in 1999 by US Space Command of responsibility for information operations signals that the military will likely integrate space-based systems into information operations.[40]

International Telecommunications Law and Information Operations

International telecommunications law is a web of bilateral and multilateral treaties.[41] The 1992 ITU Convention[42] is the preeminent treaty in this area, with over 130 signatories. This convention and others established the International Telecommunications Union (ITU), a specialized agency of the United Nations with the authority to formulate telegraph and telephone regulations which become binding legal obligations after formal acceptance by ITU members.

Article 45 of the ITU Convention states 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 other duly authorized operating agencies, which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations."[43] Annex 2 of the Convention defines harmful interference as "interference which

endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations."[44] The DoD/GC Paper recognizes that jamming or spoofing a radio navigation service would violate this provision.[45] Therefore, the ITU Convention and the entire telecommunications multilateral treaty regime would seem to limit information operations that involve interference with radio broadcasting.

Still, as the paper notes, Article 48 of the ITU Convention provides an exemption for military operations: "Members retain their entire freedom with regard to military radio installations of the Army, Naval, and Air Forces."[46] Article 48 continues, "[n]evertheless, 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."[47] The DoD/GC Paper also notes that, in July 1994, the Department of Justice's Office of Legal Counsel relied on Article 48 in deciding that the United States could broadcast messages to the Haitian people from military aircraft and international air space urging them not to flee Haiti by sea in hazardous vessels.[48]

The ITC also allows signatory States to interfere with international telecommunications in certain circumstances. Article 34 allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its 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."[49] In addition, States may "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."[50] And finally, Article 35 allows members "to suspend the international telecommunications service for an indefinite time, either generally or only for certain relations and/or for 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."[51] The ITC provisions do not state whether the treaty applies during armed conflict. However, as the DoD/GC Paper notes, there is precedent that international communications treaties are suspended during armed conflict. During World War I, for example, the British Navy cut Germany's major submarine cables despite the existence of the 1884 Convention for Protection of Submarine Cables. It should be noted, however, that the United States may have entered into bilateral communications agreements with particular

countries that may be relevant depending on the circumstances of a particular information operation.

The DoD/GC Paper concludes by stating that "International Communications Law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peace time."[52] However, US information operations may be carried out not only by military forces, but also by intelligence personnel engaged in covert action or other intelligence-related activities. Yet, the ITU Convention's Article 48 exemption for military operations does not appear to allow for such interference in telecommunications by non-military personnel such as intelligence operatives.[53] Also, the international telecommunications treaty regime contains certain notice provisions, and it is unlikely that the military would wish to publicize its information operations in that way.

A Checklist of Other US Treaty Obligations

In addition to international law governing the use of outer space and telecommunications, various other treaties and international obligations could impact upon, interfere with, and possibly even prohibit the conduct of US information operations. The following discussion is intended as a non-exhaustive checklist for decisionmakers faced with the question of whether to authorize a particular information operation.

The United Nations Convention on the Law of the Sea (LOSC)

This convention, which is currently under review by the Senate for advice and consent, codifies several provisions of customary international law and creates new requirements. One such provision of preexisting customary international law is Article 19, which states that a vessel exercising the right of innocent passage through another nation's territorial sea cannot engage in activities "prejudicial to the peace, good order, or security of the coastal State."[54] Article 19 defines "prejudicial activities" to 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 defense or security of the coastal State;

- Any act of propaganda aimed at affecting the defense 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[.][55]

While the DoD/GC Paper observes that LOSC provisions "have the potential to affect only a narrow category of information operations,"[56] a literal reading of the LOSC seems to point to information operations falling under its purview. Ship-borne information weapons could be classified as "prejudicial to the peace, good order or security of the coastal State" because information operations are "aimed at interfering with particular systems of communication or other facilities or installations of the coastal State." The Convention establishes a nation's maximum territorial sea as twelve miles from the nation's coast, significantly smaller than the 200 miles that particular nations claim.[57] Thus, an obvious remedy for any legal problems with ship-borne information operations is for ships wielding information weapons "against" or otherwise "aimed at" a coastal nation to stay outside of the twelve-mile limit. It should be noted that the LOSC does not expressly address whether its obligations are enforced during an international armed conflict.

Treaties on Civil Aviation

Article 3(d) of the 1944 Chicago Convention, which established the International Civil Aviation Organization (ICAO), states, "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."[58] The DoD/GC Paper observes that, as a result, military aircraft have an obligation of "due regard" for the safety of civil aircraft, meaning an obligation "not to interfere with the systems" of civilian aircraft, but does not elaborate on this obligation.

A question thus arises concerning the use of information warfare against particular navigational systems or other dual-use systems, i.e., used both by military and civilian aircraft. For example, a particular navigational satellite might be used both by military and civilian aircraft, or a particular civilian–military airport might use the same radar for both military and civilian flights. An information operation against such computer equipment with the aim of disrupting military operations could impact civilian aircraft as well, leading to a violation of civil aviation treaty obligations. The DoD/GC Paper notes that the Chicago Convention specifically provides that the treaty does not "affect the freedom of action of any of the contracting States affected,

whether as belligerents or as neutrals."[59] It also notes that many provisions of the convention are inconsistent with wartime circumstances and, therefore, the Chicago Convention would be unlikely to survive as a complete entity in the event of an armed conflict. However, Article 89 does not provide adequate guidance in ascertaining what provisions of the Chicago Convention are applicable during an armed conflict and thus what limitations exist on information operations in wartime.

Treaties on Diplomatic Relations

The 1961 Vienna Convention grants to diplomatic missions the right of inviolability of the premises and its documents and communications. The convention also requires that diplomatic personnel respect the laws and regulations of the State in which they are stationed and that "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 State and the receiving State."[60] As the DoD/GC Paper concludes, "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."[61]

Treaties of Friendship, Commerce and Navigation (FCN)

These bilateral agreements between the United States and other nations establish arrangements for tourism, trade, transportation, and other routine and practical issues. According to the DoD/GC Paper, such treaties probably would be suspended in the event of armed conflict. However, to the extent that information operations are utilized in peace-time, decisionmakers must take into account obligations incurred in FCN treaties to the extent they will impact information operations. For example, one could imagine the scenario in which the targeted nation will attribute the information operation to criminal elements or to economic espionage and will request assistance from the United States under the FCN treaty (or under mutual legal assistance agreements and extradition agreements)in response to such information operations. US officials need to be prepared to respond to such a request even when the information operation is a military or intelligence operation.

Status of Forces Agreements and Foreign Domestic Law

Stationing agreements and defense cooperation agreements memorialize the consent of the host nation to the presence of US troops, set limits on troop numbers, and identify facilities. The United States also commonly enters into status of forces agreements (SOFAs) to address legal jurisdiction over its forces. The DoD/GC Paper notes that, by the end of 1998, the United States was a party to 103 SOFAs. Many require that the US notify the host nation of any significant change regarding the capabilities or status of the military forces stationed in the host country.

As the DoD/GC Paper states, if authorities intend to conduct information operations from US bases abroad, a determination must be made as to whether the relevant agreements require notifying the host nation and perhaps even requesting its consent.[62] The paper also notes that such agreements often require that US equipment not interfere with the host nation's communication system and that such equipment cannot violate the host nation's laws and regulations. Host nations may understandably be concerned about information weapons criss-crossing their telecommunications equipment for fear of possible, unintentional infection of the host nation's computers. They might also be wary of the counter-measures or acts of self-defense by the target nation of a US information operation. Yet, even if a host nation opposed the use of US forces stationed in its country to conduct information operations, the difficulty of attributing an information operation to its true source might give US forces sufficient cover regarding the origin of the attack, and thus might assuage the host nation's concern regarding its own possible vulnerability to counter-measures or reprisals.

It should be noted that foreign domestic laws impact the conduct of US defensive information operations because foreign law enforcement officials may not be authorized to conduct criminal investigations of possible computer crime or information warfare unless the conduct at issue constitutes a crime according to the laws of that particular country. As a result, officials may not receive the expected levels of cooperation from foreign law enforcement officials in the investigation of an apparently criminal information operation emanating from a particular country. Conversely, if a foreign government does outlaw activity that constitutes information warfare, US military officials may decide to refrain from offensively-oriented information operations conducted from their bases in that particular country in order not to subject US forces to liability or culpability for violating that foreign country's laws. Furthermore, even if US forces would not be liable or culpable legally, commanders may wish to avoid the appearance of violating foreign domestic law.[63] As the DoD/GC Paper notes, conduct by

military personnel that constitutes an offense under the host nation's law and not under US law could give the host nation exclusive jurisdiction to prosecute. This situation could occur if a host nation's computer law is more developed than US law or prohibits particular forms of information warfare.[64] Of course, the flexibility and interconnectedness of the Internet mean that the United States could conduct the information operations from a host country that allows such operations, thus avoiding the particular countries that criminalize such activity.[65]

Espionage

The DoD/GC Paper emphasizes the fact that, given the ambiguity surrounding the concept of information warfare, the division between espionage and the use of force is ambiguous. Thus, it may be unclear whether an information operation constitutes espionage or a military attack—or both. The paper also notes that the division of labor between the intelligence community and the military concerning covert action is likely to be blurred by information operations. As it concludes, "it remains to be seen how information operations activities will fall within this division of labor," especially when such information operations occur in the context of military operations other than war such as peacekeeping, peace-enforcement, and counter-narcotics missions.[66]

An Information Warfare Treaty?

In October 1998, Russia introduced a resolution in the United Nation's First Committee calling for States to report their views concerning the "advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons." The United States responded that it was premature to discuss negotiating an international treaty concerning information warfare. On the one hand, an international treaty serves the interest of less-technologically developed nations because the treaty would most likely restrict more advanced nations such as the United States from developing information warfare techniques. On the other hand, an international treaty need not necessarily set restrictions below the level at which advanced nations currently operate. Such restrictions would be equivalent to arms-control agreements setting a limit on number of weapons well-above the number of weapons actually possessed by signatory States. Furthermore, a treaty limiting information operations by nations does not address the problem of terrorists or hackers.[67]

A treaty could potentially ban information operations but allow research on information warfare or limit research to defensive capabilities. However, the

distinction between offensive and defensive information warfare might blur because an understanding of offensive operations is required for construction of effective defenses (and vice versa).[68] Alternatively, a treaty could conceivably require certain identifying marks on military information operations so that countries can identify the source of operations, although the lack of such attribution characteristics might be a violation of the current law of war concerning perfidy—meaning that a new treaty is not required for this specific purpose. It should also be noted that, as a nation advances technologically, it becomes more vulnerable to technological attack; in other words, the United States could actually benefit from an international treaty due to its economy's heavy reliance on computer infrastructure. This assumes, however, that the treaty is both widely adopted and enforceable. Also, the treaty should not leave the United States powerless to defend itself against attacks from terrorists or hackers as opposed to information operations launched by another State.

The DoD/GC Paper concludes that "[t]here seems to be no particularly good reason for the United States to support negotiations for new treaty obligations and most of the areas of international law that are directly relevant to information operations."[69] It nevertheless observes that one area in which international agreements would be beneficial is cooperation concerning criminal law, namely efforts to raise the level of foreign countries' criminal laws concerning computer crimes to that recognized by the United States. Although the DoD/GC Paper states that it is unclear how such a treaty could actually work in practice, it also speculates that a treaty concerning information terrorism might be useful.

Conclusion

The DoD/GC Paper states that there are no "show-stoppers" in international law prohibiting US information operations.[70] However, obligations concerning the use of outer space may present problems if a particular information operation qualifies as a "weapon of mass destruction." Furthermore, other obligations under international law present complications—and opportunities—for the conduct of US information operations. Decisionmakers must be sure to assess the impact of international law on each proposed information operation.

Notes

1. WILLIAM SHAKESPEARE, KING HENRY THE SIXTH, act II, scene i, *in* WILLIAM SHAKESPEARE: THE COMPLETE WORKS (Alfred Harbage ed., 1969).

2. Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. This paper is appended to this volume as the Appendix. All cites are to Appendix pagination.

3. The law of war includes such general principles as the distinction of combatants from noncombatants, military necessity, proportionality, and the outlawing of indiscriminate weapons and perfidy.

4. Article 2(4) of the UN Charter requires signatory States 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." UN CHARTER art. 2, para. 4, 59 Stat. 1031, 1037. The Charter also permits the Security Council to authorize coercive measures, such as military force, in the event that there is a "threat to the peace, breach of the peace, or act of aggression." *Id.*, art. 39, 59 Stat. 1043. Article 51 provides that "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. *Id.*, art. 51, 59 Stat. 1044–45. The DoD/GC Paper concludes that "[a] close parsing of the language would tend to limit its effect to attacks and invasions using traditional weapons and forces." DoD/GC Paper, *supra* note 2. However, the paper does not explicate the opposing view, namely that an armed attack may not mean *only* an armed attack in a traditional sense, but also may include information warfare because information operations can lead to property destruction and the loss of life. Still, the paper goes on to state that 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." *Id.* In other words, even if information operations might not constitute an armed attack under the language of Article 51, States might have a right of self-defense in response to information warfare attacks based on a more expansive right of self-defense that existed prior to the UN Charter.

5. *See also* Todd Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 567–600 (Spring–Summer 1998); Richard W. Aldrich, The International Legal Implications of Information Warfare (US Air Force Academy, Institute for National Security Studies, 1995); Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272 (1996).

6. *See generally*, LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW (1997).

7. *See generally*, THE INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Stuart J.D. Schwartzstein ed., 1996). *See* THE INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Ryan Henry & C. Edward Peartree eds., 1998).

8. *See generally*, IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE, (John Arquilla & David Ronfeldt, eds., 1997); DAVID A. OCHMANEK, EDWARD R. HARSHBERGER, ET AL., TO FIND AND NOT TO YIELD: HOW ADVANTAGES IN INFORMATION AND FIREPOWER CAN TRANSFORM THEATER WARFARE (1998). *See also* BRIAN NICHIPORCK & CARL H. BUILDER, INFORMATION TECHNOLOGIES AND THE FUTURE OF LAND WARFARE (1995).

9. Prosenjit Bhattacharya, *The Next Wars in Space, Cyberspace*, FOREIGN ECONOMIC TIMES, Dec. 21, 1999. One advantage that western countries have in terms of facing information warfare attacks is that they have already been targeted themselves by their own children, namely teenage hackers who constantly probe governmental and other key computer systems for weaknesses. In essence, these teenage hackers keep governmental and industry leaders who are charged with defense against information warfare on their toes, resulting in hardened defenses that have as a

secondary benefit increased defensive capability against foreign attackers. *See* Interview with Jarod Lanier, CNN (Jan. 9, 2000).

10. Winn Schwartau, *An Introduction to Information Warfare, in* WAR IN THE INFORMATION AGE: NEW CHALLENGES FOR U.S. SECURITY 49 (Robert L. Pfaltzgraff, Jr. & Richard H. Shultz Jr. eds., 1997).

11. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998).

12. *Id.* at I-11.

13. *Id.* at I-9.

14. *See Washington Outlook,* AVIATION WEEK AND SPACE TECHNOLOGY, Dec. 6, 1999, at 27.

15. Robert Burns, *Pentagon Cites Cyber Warfare Report, AP Online,* Nov. 9, 1999.

16. David A. Fulghum, *Telecom Links Provide Cyber-Attack Route,* AVIATION WEEK AND SPACE TECHNOLOGY, Nov. 8, 1999, at 81–83. While the Iraqi telecommunications network was severely attacked during the Gulf War by Coalition air forces, Yugoslav telephone and Internet links apparently went relatively unscathed. Some analysts have postulated that this was a deliberate move by NATO in order to maintain pathways for US military hackers to enter Yugoslav computers. An after-action survey of bombing damage done by William Arkin, an independent defense analyst, found that only 3 of about 30 Serbian telephone system nodes had been attacked by NATO aircraft and that none of the three network control stations for cell phone usage had been attacked, even though Yugoslav agents were reportedly phoning in with the times of NATO aircraft departures from NATO bases. Arkin speculated that NATO forces deliberately did not attack these communications nodes in order to maintain pathways for information operations. *Id.*

17. *See* Bradley Graham, *Military Grappling with Rules for Cyber Warfare,* THE WASHINGTON POST, Nov. 8, 1999, at A1.

18. *See* Michael Evans, *War Planners Warn of Digital Armageddon,* THE TIMES OF LONDON, Nov. 20, 1999, at 11.

19. *See* MND Calls for Establishment of High-level Defense Mechanism, Central News Agency of Taiwan, Nov. 2, 1999.

20. *Bringing the Internet into the Military System is of Equal Significance with Land, Sea, and Air Power,* LIBERATION ARMY DAILY, Nov. 1999.

21. Robert Karniol, *Briefing-Military Modernization in Asia,* JANE'S DEFENSE WEEKLY, Nov. 24, 1999.

22. *See* DoD/GC Paper, *supra* note 2.

23. *See id.*

24. *Id.* This is even more true with the growing use of commercial satellite imagery. *See* Ann M. Florini & Yahya Dehganzada, *Commercial Satellite Imagery Comes of Age,* ISSUES IN SCIENCE AND TECHNOLOGY, Fall 1999, at 45–52.

25. DoD/GC Paper, *supra* note 2.

26. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

27. Agreement on the Rescue of Astronauts, Return of Astronauts, and the Return of Objects Launched into Outer Space, April 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119 [hereinafter Rescue and Return Agreement].

28. The Convention on International Liability for Damages Caused by Space Objects, March 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention].

29. The Convention on the Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention].

30. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *opened for signature* Dec. 18, 1979, 1363 U.N.T.S. 22. The Multilateral Prohibition of Military and

other Hostile Use of Environmental Modification Techniques, signed in 1977, contains some provisions applying to space activity, but these are not relevant to information operations. *See* DoD/GC Paper, *supra* note 2.

31. DoD/GC Paper, *supra* note 2. *See* MICHAEL J. MUOLO, SPACE HANDBOOK: A WAR FIGHTER'S GUIDE TO SPACE 53–57 (1993).

32. Outer Space Treaty, *supra* note 26, art. IV, 18 UST. 2413–14, 610 U.N.T.S. at 208.

33. *Id. See also* DoD/GC Paper, *supra* note 2. The 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Limited Test Ban Treaty) prohibits nuclear explosions in outer space (Aug. 5, 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43).

34. Limitation of Anti-Ballistic Missile Systems Treaty, May 26, 1972, art. V, US-USSR, 23 U.S.T. 3435, 3441.

35. *See* DoD/GC Paper, *supra* note 2.

36. Outer Space Treaty, *supra* note 26, art. IV.

37. *See* Byard Q. Clemmons, *Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction*, MILITARY REVIEW, Sept.–Oct. 1999, at 35–45.

38. *See id.*

39. *See* DoD/GC Paper, *supra* note 2.

40. *See generally*, THE US AIR FORCE IN SPACE: 1945 TO THE TWENTY-FIRST CENTURY (R. Cargill Hall & Jacob Neufeld eds., 1998); AIR AND SPACE POWER IN THE NEW MILLENNIUM (Daniel Goure & Christopher M. Szarza eds., 1977); MUOLO, *supra* note 31, vol. I & II.

41. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885–937 (1999).

42. Constitution and Convention of the International Telecommunication Union, Dec. 22, 1992, S. Treaty Doc. No. 104–34. (1996) [hereinafter ITU Convention].

43. *Id.*, art. 45.

44. *Id.*, Annex 2.

45. *See* DoD/GC Paper, *supra* note 2. The paper makes reference to the articles as numbered in the 1982 International Telecommunication Convention, the predecessor of the ITU Convention of 1992. The substantive content of the articles in both conventions is the same.

46. ITU Convention, *supra* note 42, art. 48.

47. *Id.*

48. *See* DoD/GC Paper, *supra* note 2.

49. ITU Convention, *supra* note 42, art. 34, S. Treaty Doc. No. 104-34.

50. *Id.*

51. *Id.*, art. 35.

52. DoD/GC Paper, *supra* note 2.

53. It is interesting to note that domestic US law concerning telecommunications, 47 US Code § 502, provides as follows:

> 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.

The DoD/GC Paper notes that the Department of Justice's Office of Legal Counsel issued a written opinion stating that 47 US Code § 502 does not apply to US military personnel acting under instructions of the President as Commander in Chief, specifically referring to the October

1993 radio messages broadcast by the US armed forces to Haitians. DoD/GC Paper, *supra* note 2. This opinion does not cover, although it does not necessarily prohibit, such operations by non-military personnel.

54. United Nations Convention on the Law of the Sea, Dec. 10, 1982, art. 19, 1833 U.N.T.S. 397, 404 [hereinafter LOSC].

55. *Id.*, art. 19 (a), (c), (d), and (k).

56. DoD/GC Paper, *supra* note 2.

57. *See* LOSC, *supra* note 54, art. 3, 1833 U.N.T.S. 400.

58. Convention on International Civil Aviation, Dec. 7, 1944, art. 3(d), 61 Stat. 1180, 1181, 15 U.N.T.S. 295, 298 [hereinafter Chicago Convention].

59. *Id.*, art. 89, 61 Stat. 1205, 15 U.N.T.S. 356.

60. Vienna Convention on Diplomatic Relations, April 18, 1961, art. 41, 23 U.S.T. 3227, 3247, 500 U.N.T.S. 95, 120 [hereinafter Vienna Convention].

61. DoD/GC Paper, *supra* note 2.

62. *Id.* at 40.

63. *Id.* at 42.

64. *Id.* at 43.

65. *Id.*

66. *Id.* at 47. For an analysis of interagency problems associated with US defensive information operations, *see* Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, COMMUNICATION LAW CONSPECTUS, Winter 1999, at 153–172. For an analysis of information operations in military operations other than war, see THE CENTER FOR ADVANCED COMMAND CONCEPTS AND TECHNOLOGY, OPERATIONS OTHER THAN WAR (OOTW: THE TECHNOLOGICAL DIMENSION) (1995), at www.ndu.edu/inss/books/ootw/ootwhome. html.

67. *See* Bill Flynt, *Threat Convergence*, MILITARY REVIEW, Sept.–Oct. 1999, at Z-11 (listing the range of sources of threats, including terrorist and hackers).

68. *See generally*, DAVID S. ALBERTS, DEFENSIVE INFORMATION WARFARE (1996), www.ndu/edu/inss/books/diw/index.html. *See also* ROBERT H. ANDERSON, PHILLIP M. FELDMAN, ET AL., SECURING THE US DEFENSE INFORMATION POSTURE: A PROPOSED APPROACH (1999).

69. *See* DoD/GC Paper, *supra* note 2.

70. *Id.*