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

XIV

Information Operations in the Space Law Arena: Science Fiction Becomes Reality

Douglas S. Anderson and Christopher R. Dooley*

The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents.[1]

War fighting has come a long way from the days of swords and shields. No longer must armed forces rely completely on "arms," or even "forces," to gain victory on the battlefield. Today, computers are becoming the weapon of choice for the military warrior. Forget the old standbys of the M-16, Abrams tank, Nimitz-class carrier, or F-16. As forces become more computer and technologically dependent, militaries of the future will have a completely different look.[2] In some respects, this should not surprise us. Technological change has always transformed the means and methods of warfare, but the *pace* of transformation has increased dramatically in the past few decades. While laptops and cyber chips may never completely displace guns and bullets in the warfighter's arsenal, they certainly will become an increasingly critical part.

Nowhere is this technological transformation more evident than in the areas of military space resources and information operations. Lasers, electronic pulses, pinpoint sensing equipment, and a vast array of other sophisticated space systems

are becoming an ordinary part of our day-to-day military experience. As the latest microchip and computer network capabilities become an integral part of attacking and defending those space systems, the future will be fraught with dramatic new possibilities. Yesterday's science fiction is becoming today's reality.

Background

This new reality is already a significant threat to the US national security infrastructure. Consider the evidence. According to former Deputy Defense Secretary John Hamre, one particular Department of Defense (DoD) computer network is penetrated as often as 10-15 times a day by computer hackers.[3] With more than 2.1 million computers and 10,000 local area networks, DoD was the target of more than 250,000 *detected* intrusions in 1998.[4] That figure is even more astounding when you consider that the Defense Information Systems Agency (DISA) estimates that only one intrusion out of every 150 is even detected.[5] In February 1998, while the US was preparing to deploy forces to the Persian Gulf, a computer attack known as "Solar Sunrise" was initiated against computer systems throughout the Department of Defense.[6] The potential implications of the attack were sobering:

> Someone, or some group of people . . . gained root access, systems administrator status, on over 20 important logistical computers throughout the Air Force and, subsequently, we learned throughout the Navy and Army. They could have therefore crashed the systems. They downloaded thousands of passwords and they installed sniffers and trap doors. And for days, critical days, as we were trying to get forces to the Gulf, we didn't know who was doing it. We assumed therefore it was Iraq. We found out it was two 14-year-olds from San Francisco. Was that good news or bad? If two 14-year-olds could do that, think about what a determined foe could do.[7]

"Eligible Receiver" was a cyber attack exercise in June 1997, which was launched by the Department of Defense against itself to see how well our systems detected and responded to the attack. For days, the attack went undetected. This exercise demonstrated the ability of a potential enemy to disrupt computer operations of major military commands, create large-scale blackouts, and interrupt emergency phone service in Washington, DC.[8] These types of cyberspace intrusions are not limited to the domain of criminals or terrorist hackers. States have been, and will continue to be, engaged in the use of information

operations. They recognize, as does the US, its value in protecting national security interests.[9] There have been reports that during the NATO-led Operation ALLIED FORCE campaign against Serbia, Serbs hacked into the NATO World Wide Web pages and flooded e-mail accounts in the US with pro-Serb messages.[10] The reported Serbian actions, and others like them, demonstrate that the threat of cyber attack is real. Both the White House and DoD are certainly convinced. In response to the threat against DoD communications systems and other government computer data, the Clinton Administration issued a White Paper in May 1998 setting forth policy and goals on critical infrastructure protection.[11] In addition, the DoD created the Joint Task Force - Computer Network Defense[12] (JTF-CND), which maintains a 24-hour operations center to provide warnings of cyber attacks on DoD systems.[13]

Couple the dangers of cyber attacks with our heavy reliance on space systems and the threat becomes all the more sobering. It is more than just an axiom that outer space is the proverbial high ground.[14] Access to, and control of, outer space are fundamental to our nation's economic and military security.[15] Moreover, we can no longer take that access and control for granted. While the US dominates outer space activity today, it is estimated that within the next 10 to 20 years more space-based systems will be available to friendly and unfriendly nations alike.[16] These systems will provide communications, weather, surveillance, and a host of other critical services that will have both a military and civilian use. Friends and foes will be able to use the same space systems.[17] Therein lies one of the dangers.

Modern military forces rely heavily on dual-use telecommunications media, including telephones, faxes, and e-mail that travel over civilian owned or operated networks. In fact, 95 percent of all DoD telecommunications traffic flows over public networks.[18] Telecommunications are a particularly acute vulnerability because of this high degree of dependence by modern militaries.[19] This reliance permeates every facet of society, thus allowing exploitation throughout the conflict spectrum at the tactical, operational, and strategic levels.[20] Because of their data transfer capacity and mobility, telecommunications are increasingly important as the critical media by which our national instruments of power are directed.[21]

The threats are real, the vulnerabilities potentially grave, and new computer technology is largely responsible. Information operations and outer space operations are uniquely intertwined through their mutual reliance on, and vulnerability to, computer technology. Moreover, that technology is changing rapidly. From a military operation or infrastructure protection perspective, it is difficult to keep pace with such rapid developments. Equally daunting is the effort to

apply existing legal regimes to these new technologies. Both information operations and space operations apply military force in a way that challenges traditional international legal norms. Admittedly, such a topic raises far more issues than can be adequately addressed here. Therefore, this chapter is intended only as a basic primer to introduce the reader to the international law applicable to information operations that affect military space systems.

Scope and Definition of the Information Operations Concept

It is readily apparent how wide-ranging the computer attack threat to our national security infrastructure can be. It can include activities such as offensive and defensive electronic jamming, information denial, manipulation of data, morphing of video transmissions, destruction of hardware, or a myriad of other techniques to render military weapons and systems ineffective, inoperable, or unavailable at a critical time. In the legal context, information operations—including threats by individuals, organizations, or nations; actions motivated by goals ranging from monetary greed to terrorist revenge; and operations with military objectives—touch both international and domestic law.

For our purposes, discussion of information operations is limited to actions by, or on behalf of, nation States. Moreover, domestic laws and regulations are not our focus, although there are certainly many regulations that apply.[22] Instead, we examine those aspects of public international law relating to outer space that may have an impact on information operations.

As a starting point, it is necessary to define terms, since "information operations" is not a term of art with a universally agreed upon meaning. Indeed, the US military services, and the DoD itself, do not use consistent terminology. For example, in the glossary of Doctrine Document 2-5, the Air Force adopts the DoD definition of "information operations" found in DoD Directive 3600.1: "actions taken to affect adversary information and information systems while defending one's own information and information systems."[23] Yet the Air Force takes the unusual step of qualifying that definition with what it calls "a more useful working definition," namely, "[t]hose actions taken to gain, exploit, defend or attack information and information systems and include both *information-in-warfare* and *information warfare* (emphasis added)."[24] Even though the Air Force and DoD definitions emphasize different aspects of information operations, their concepts, as well as that of the other military services, include both offensive and defensive operations. While we use the term "information operations" in a very broad sense that includes attacking or

defending information and information systems, for the purpose of this chapter we place particular emphasis on computers as the primary means of doing so.

The Importance of IO to Military Operations

The electron may well be the ultimate precision guided weapon,[25] for information is becoming a strategic resource that could prove as valuable and influential in the post-industrial era as capital and labor were in the industrial age.[26] Use of the term "information operations" signifies a new way of thinking that recognizes the central importance of modern information systems as force enhancers, as vitally important targets, as a means of defense, and as cyberweapons that may be used to attack certain targets.[27]

> While both netwar and cyberwar[28] revolve around information communications matters, at a deeper level they are forms of war about "knowledge"—about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.
>
> Netwar refers to information-related conflict at a grand [strategic] level between nations or societies. It means trying to disrupt, damage or modify what a target population "knows" or thinks it knows about itself and the world around it. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, and efforts to promote a dissident or opposition movement across computer networks.[29]

Daniel Kuehl, Professor of Military Strategy at the National Defense University's School of Information Warfare and Strategy, notes that information warfare is intended to "influence the enemy's will and ability to fight so that they stop fighting and you win."[30]

> Information is aimed at affecting the enemy's cognitive and technical abilities to use information while protecting our own—to control and exploit the information environment. In some ways it is technologically independent in that operations can be conducted in any of the media of war, not just cyberspace, to attain that key objective of weakening the enemy's will, but in other ways the new medium of cyberspace offers a particularly rich environment through which we can reach those elusive targets, the enemy's will and capability, via the various

> entry ways and connecting points in the information environment, whether they be hardware, software, or wetware [the human mind].[31]

The objective of offensive warfare has always been to deny, destroy, disrupt, or deceive the enemy—either in its employment of forces or in retaining the support of its people.[32] Mao Tse-Tung believed that "to win victory we must try our best to seal the eyes and ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders."[33] Information operations are particularly well suited to sealing the eyes and ears of the enemy. By disrupting or denying the flow of information between the enemy's military forces and its command and control elements, information operations can essentially render sightless any enemy commander.[34]

The Importance of Space Systems to Military Operations

Space denial is an important tenet of our national defense strategy.[35] Inherent in that tenet is the recognition that control of outer space is essential for victory on today's battlefield. Certainly, space power has evolved over the last ten years from merely being a useful force multiplier to being no less than an "indispensable adjunct."[36] According to one author, "the contemporary reality is that the US armed forces could not prevail, even against a modestly competent foe, without the support of space systems."[37] Air Force Chief of Staff General Michael E. Ryan gives an excellent example of the practical use of space assets in a deployed environment.

> When a U-2 reconnaissance aircraft goes on a mission, the planes can send raw surveillance data via satellite to intelligence specialists in the United States, who can analyze it and send it to Operation Allied Force's Combined Air Operations Center at Vicenza, Italy. The data can then be sent to a pilot flying a strike mission. All this can be done within minutes and reduces the number of airmen who have to deploy.[38]

During Operation ALLIED FORCE in the Balkans, a variety of space assets were used to support the NATO effort. According to Brigadier General Mike Drennan, Commander of the 21st Space Wing at Peterson Air Force Base, Colorado, navigation, strike indicators, search and rescue, communications, and weather images represented just some of the space systems support provided to commanders in the theater.[39] Additionally, both conventional air-launched cruise missiles and Tomahawk land-attack missiles launched from ships, as well as certain other precision guided weapons, owed their success to the Global

Positioning System (GPS).[40] While GPS was designed by the Department of Defense as a dual-use system, its primary purpose has been to enhance the effectiveness of US and coalition military forces.

Our national space policy expressly recognizes that US national security is dependent upon an ability to maintain access to, and use of, space.[41] At times, our national security interests may require denial of space to our adversaries. Information operations can play a key role in space control and denial. For instance, intrusions into an adversary's computer network and manipulation of key data can prevent a space launch, move an opponent's communications or remote sensing satellites out of orbit, or preclude satellite data from reaching command and control centers.

World Wide Availability of Space Data Information

One of the realities of space denial and space control objectives within our national space policies and military doctrine is that the US does not, and will not, have exclusive access to space. A growing number of nations and organizations are obtaining space assets and systems of their own.[42] China has a rapidly developing space program, as does Japan, India, Brazil, and, of course, Russia.[43] France, India, and Israel have capabilities in high-resolution satellite surveillance technology, and this type of data is now commercially available for purchase by any nation.[44] The US Landsat and the French SPOT [*Systeme Pour l'Observation de la Terre*] imaging systems have been around for years, but their technology continues to improve and become more widely available.[45] For instance, the French are currently marketing ten-meter resolution images, while some commercial satellites are now capable of one-meter resolutions.[46] More recently, the European Space Agency has developed Earth Resources Satellites (ERS) 1 and 2, and marketed their synthetic aperture radar (SAR) images. Canadian Radarsat and the Helios reconnaissance satellite owned by France, Spain, and Italy may also have future commercial availability.[47] A further example of the public commercial availability of space system technology is the US' hugely successful GPS, which, until recently, enjoyed a near monopoly in space-based navigation technology. Besides the availability of GPS, Europe is planning to launch its own satellite navigation system called Galileo, projected to be operational in 2008.

As non-US satellite navigation systems are developed and launched, additional legal issues and national security concerns arise. When a virtual US monopoly on particular space systems exists, such as there used to be with GPS, space denial or control is merely a matter of interrupting or encoding the information from our own systems so that other nations are unable to use it.[48]

However, when other nations have similar space systems, or can purchase the information they produce, space denial or control may require more aggressive means of information operations. The commercial availability of potentially sensitive data creates obvious risks to national security. According to one analyst, "Islamic Jihad could get its hands on a one-meter resolution picture of a US Air Force General's headquarters in Turkey, convert the shot to a precise three-dimensional image, combine it with data from a GPS device, and transmit it to Baghdad, where a primitive cruise missile, purchased secretly from China could await its targeting coordinates."[49]

Information operations, used to assure US space control by denying its use by others, will certainly raise eyebrows and stir heated debate in the international community. Since any decision to employ a military option, especially one affecting outer space or space systems, must weigh political concerns and sensitivities, a consideration of world opinion on the subject is useful.

International Opinion on the Weaponization of Space

Since the Soviet launch of Sputnik in 1957, many nations in the world community have been ardently concerned about preventing the placement of weapons in outer space, particularly with respect to new weapons technology. As a result, any potential use of offensive information operations in, or affecting, outer space will likely aggravate international concerns.

The debate has been polarizing, frequently pitting practical national security objectives against the desire to maintain at least one environmental realm free from military conflict. Early UN General Assembly resolutions generally sought to provide that outer space would be used exclusively for "peaceful purposes," but the term was never defined.[50] While nearly all voices claimed to be in favor of peaceful purposes, they were not so harmonious on the degree of military activity that concept included. The reality, of course, is that outer space has been a domain of the military since 1957 and has been of significant importance to the military to the present day. Today, some advocates of the non-weaponization of space seek to impede further military development of space with the ultimate hope of curtailing an arms race in outer space. While opponents of this view are not against "peaceful purposes" per se, they stress the need to be prepared for war as the best way to protect national interests.[51] In general, the two views are irreconcilable, although there is room for agreement on specific issues.

The United Nations, which includes members on both sides of the debate, has taken an active role in international space law from the very inception of the

space age. It has done so primarily through the work of the Committee on the Peaceful Uses of Outer Space (COPUOS).

Committee on the Peaceful Uses of Outer Space

In 1959, the United Nations established COPUOS[52] to enhance international cooperation in the peaceful uses of outer space. Since its creation, it has been the primary forum for the development of international space law. In fact, COPUOS was the architect for each of the existing five space law treaties. Of those, four have been ratified by most space-faring nations; together, they comprise the core body of international space law.[53]

From its inception, COPUOS has promoted the use and maintenance of outer space for peaceful purposes. Early work resulted in the adoption of General Assembly Resolution 1721 on December 20, 1961, which stated that "the common interest of mankind is furthered by the peaceful uses of outer space."[54] General Assembly Resolutions 1884 and 1962, adopted two years later, continued that theme.[55] Today, the Committee continues to encourage research and distribution of information on outer space matters, sponsor various programs and conferences, and study the legal issues arising out of space exploration and activity.[56]

As its name implies and its work confirms, COPUOS starts from the premise that outer space should be maintained for "peaceful uses." While this is a term that everyone has adopted, as noted earlier, there is strong disagreement about its meaning. Past practice has demonstrated that most COPUOS members believe military activity in outer space, as potentially contrary to the goals of international peace and security, must be closely scrutinized. In fact, at its fifty-first session, the UN General Assembly passed Resolution 51/44, "Prevention of an arms race in outer space." Included in that resolution was the statement that the General Assembly recognizes "that prevention of an arms race in outer space would avert a grave danger for international peace and security."[57] Other General Assembly resolutions contain similar language.[58]

The large number of early space treaties and General Assembly resolutions would ordinarily reflect a committee that works well together. However, that has not been the case with COPUOS. Its early success in obtaining the first four treaties was due largely to the fact that compromises on space issues were easier to obtain before the full potential of space exploration had been fully understood.[59] However, fundamental rifts soon developed within COPUOS, and have continued, between space and non-space powers.[60] More recently, the United States has found itself on the minority side of several General Assembly resolutions intended to de-militarize outer space.

From the perspective of the UN Charter, these resolutions are merely non-binding recommendations.[61] However, some commentators have asserted that the "peaceful use" of outer space concept reflects customary international law,[62] and, to the extent it is referenced, therefore believe the General Assembly resolutions contain legally binding principles.[63] This argument is not particularly helpful since it does not address the meaning of the peaceful use concept. A more practical concern about these resolutions is whether the underlying viewpoint will ultimately lead to the development of another space law treaty which significantly limits military activity, including information operations, in or transiting outer space.

Conference on Disarmament

Closely related to COPUOS is the Conference on Disarmament (CD). Also a creation of the United Nations, it was established in 1979 as the single multilateral disarmament negotiating forum of the UN. The CD has grown from its original membership of 40 nations to 66, including the United States.[64] As with COPUOS, disagreements between CD members exist. These differences were clearly evident in 1985 when an Ad Hoc Committee, formed to find a means to curtail the arms race in space, held 20 meetings over a three-month period without reaching agreement on any of their objectives.[65] The primary catalyst in forming the Ad Hoc Committee was the US "Strategic Defense Initiative" program.[66] In debating a proposal for an arms control treaty for space, the United States argued that there was no need for such a treaty since existing treaties were sufficient. In contrast, the former socialist block nations indicated a willingness to conclude an agreement that would not only prohibit space attack weapons then under development, but would also require the destruction of existing weapons. While the Soviet Union accused the United States of "disrupting" and "hampering" the ratification of several important arms control agreements, China's tone was at least as emphatic. China made it clear that "the 'Star Wars' plan must not be carried out" and that "China is firmly opposed to an arms race in outer space . . . and proposes to achieve first 'the de-weaponization of outer space' at the present stage."[67] The nonaligned and neutral States consistently supported the idea that space weapons must be prevented in outer space at all costs.[68]

A more recent example of this split of opinion is found in General Assembly Resolution A/52/37, passed in 1997. That resolution called on the CD to re-examine the idea of establishing another Ad Hoc Committee to address the issue of militarization of space. This issue had re-captured the interest of the CD

in light of recent developments in lasers and perceptions that the US was seeking to weaken the Anti-Ballistic Missile (ABM) Treaty.[69] Despite the efforts and objections of the US, the resolution was supported by 128 nations, including China, Russia, Canada, Japan, Australia, and New Zealand. The US, Great Britain, and France were among the 39 abstentions.[70] Even more recently, another General Assembly resolution called for the CD to reestablish the prior Ad Hoc Committee on the Prevention of an Arms Race in Outer Space. Adopted on December 4, 1998, by an overwhelming vote of 165 to 0, the US was one of four abstentions.[71]

China has been particularly active in the CD in its efforts to keep outer space weapon-free. In addition to co-sponsoring several UN General Assembly resolutions, it has also sought to obtain a legally binding international agreement to ensure outer space remains free of all weapons. In fact, China published a White Paper in July 1998 to outline its views on the weaponization of outer space.[72] According to this paper, "China stands for the complete prohibition and thorough destruction of weapons deployed in outer space."[73] Additionally, it seeks a "ban on the use of force or conduct of hostilities in, from, or to outer space." China also wants to preclude all countries from experimenting with any space weapons systems that would provide strategic advantages on the ground.[74] While its latest White Paper does not refer to information operations, the principles outlined therein seem to imply that China would oppose the use of information operations that could be seen as a "use of force," the "conduct of hostilities," or as "a weapon of any kind" in outer space. Despite this strong language, it is not surprising to read China's most recent statements, which express an intention not only to use information operations for military purposes, but to extend their use into space.[75]

During its 1998 session, the CD included in its agenda the frequently revisited topic of the "prevention of an arms race in outer space."[76] During that session, Canada proposed that the CD create an Ad Hoc Committee, referred to earlier, with the mandate to negotiate a convention for the non-weaponization of outer space.[77] The Canadian proposal makes two important admissions. First, it recognizes that currently there is no multilateral international agreement that prohibits the deployment of weapons in outer space other than weapons of mass destruction. This recognition is consistent with the longstanding US position. Even more important, however, is the statement that "[w]e acknowledge that there is currently no arms race in outer space. We accept the current military uses of outer space for surveillance, intelligence-gathering and communications."[78] Despite these two major concessions, it is nonetheless clear that much of the world disagrees with current US national and DoD space policy to the extent that it does not expressly denounce the weaponization of outer space.

US and DoD Space Policies

The Clinton Administration announced the latest version of the National Space Policy on September 19, 1996.[79] The National Security Space Guidelines include the principle that the US will conduct its space activities in a way that assures hostile forces cannot deny our use of space and preserves our ability to conduct both military and intelligence space-related activities. This makes some in the international community uneasy.[80] The National Space Policy also makes clear what has been obvious for quite some time—that access to and use of space "is central for preserving peace and protecting US national security."[81]

In terms of information operations, nothing in our current policy prohibits or even limits use of such technology to support our space security guidelines. In fact, it obligates the DoD to "protect critical space-related technologies and mission aspects,"[82] and maintain the capabilities to execute traditional mission areas of space support, force enhancement, space control, and force application.[83] The use of information operations to protect our communication systems and data links, while being able to interfere with the communications and data of adversaries, is wholly consistent with National Space Policy guidelines.

Assurance of space access by the US is also included in the Department of Defense's new space policy set forth in DoD Directive 3100.10.[84] Announced on July 9, 1999, this policy not only echoes the guidance of the National Space Policy, it also specifically refers to the need to maintain "information superiority."[85] Moreover, the wide variety of information operations that could be used to defend against attacks upon our space systems and to assure space control is consistent with it.

Recalling the position of many nations involved in COPUOS and the CD, many of the US national and Department of Defense space policy statements may run counter to the concept of de-militarizing space.[86] Perhaps most significantly, the first sentence of the DoD policy unequivocally announces that "space is a medium like the land, sea, and air within which military activities shall be conducted."[87] Many nations represented in COPUOS and the CD do not view outer space as analogous to "the land, sea or air," but rather more like Antarctica, where they have expended much effort to exclude nearly all military activities.

When the statements of scholars and politicians from other nations are compared generally to those in the US, a clear difference of opinion regarding the proper role of the military in space, including the use of information operations, emerges. While information operations may or may not be consistent with international opinion, they are consistent with both the national and

DoD space policies. Having considered world opinion on the issue, we turn to the applicable international law as it relates to information operations in or transiting space.

Overview of Space Law Applicable to Information Operations

There currently exist no "thou shalt nots" in space law which specifically refer to the term or concept of "information operations." In fact, there are very few *specific* military activities of any kind that are restricted or prohibited.[88] For instance, one will not find among the current space law treaties any specific reference to space lasers, anti-satellite weapons, kinetic energy guns, or information operations. For the most part, when examining space law provisions, a legal practitioner needs to work with general principles that must be applied on a fact-specific basis. Therefore, we will focus on those laws having a general application to the concept of information operations and then apply them to specific scenarios.

One means of using information operations to protect our national security interests in space is by controlling our adversaries' access to information through techniques that will interrupt, interfere with, or deny critical satellite data. At times, this can be particularly sensitive since denying data to an adversary that does not own its own space system may require disrupting a third party's space system. This, in turn, may disrupt access to data for other users who may not be involved in the conflict with the US. Using information operations for such a purpose requires careful consideration of the law as well as national policy and security interests.

US Policy on GPS Data Interference

One such national policy relates to the use of US GPS data. GPS data can be accessed in two ways. The first is through the normal operation mode of the standard positioning service (SPS). This method allows access by all users, but it also enables the US to downgrade the data provided to certain users through use of various degradation technologies and cryptography. The second means of access is the GPS Precision Positioning Service (PPS), which is granted only to DoD users and enables them to receive a clear signal with properly encrypted GPS receivers. Thus, the US military could seek to intentionally impair the navigational signals released by its global navigation system in the SPS mode to protect national security interests.[89] Such interference would only temporarily prevent commercial users and others from obtaining the same quality of

information the US needs for its military operations. It would also be preceded by a public notice warning other users of the intentionally impaired signals. Since this particular GPS belongs exclusively to the US, the United States can set appropriate limits on its use by third parties.

However, on March 29, 1996, the Clinton Administration announced a new national policy that would eventually remove prior military restrictions on the management and use of the US-owned GPS. As part of that new policy, the US committed itself to "discontinue the use of GPS Selective Availability (SA) within a decade in a manner that allows adequate time and resources for our military forces to prepare fully for operations without SA."[90] The policy also stated that GPS would be provided free of charge to the rest of the world for peaceful uses on a continuous basis.

This current policy should not unduly limit DoD information operations activities designed to impair or interrupt US GPS signals when necessary. By its terms, the policy allows the US to continue selective availability measures until alternative measures allow military forces to operate without them, even if the data is used for peaceful civil, commercial, and scientific purposes. Secondly, the policy directs the DoD to develop measures to prevent the hostile use of GPS,[91] including defensive information operation measures. Finally, in the case of actual armed conflict, this internally imposed policy decision would not preclude military use of information operations to affect an adversary's ability to use the GPS system, if deemed necessary for national security purposes.

United Nations Treaties and Pronouncements

1. Outer Space Treaty

Although it was not the first international agreement to refer specifically to outer space,[92] the Outer Space Treaty which entered into force on October 10, 1967, [93] has become the cornerstone multilateral agreement dealing with the use of space. Frequently described as the "Magna Carta" of outer space,[94] its significance cannot be over emphasized. It provides the basic framework of international space law, incorporated many of the principles set forth earlier in the non-binding 1963 Declaration of Principles,[95] has been the basis of subsequent space law treaties, and contains several provisions that have general application to information operations.

Article I(1) obligates parties to use outer space "for the benefit and in the interest of all countries" and provides that it is "the province of all mankind." Some scholars have asserted that this language means that States cannot encroach upon, or interfere with, the lawful activities of other States.[96] This language does not, however, impose any legal constraints on military operations properly authorized

under international law. For example, military action pursuant to a Chapter VII Security Council resolution is, of course, an authorized activity for the benefit and in the interest of all countries, given the UN's authority to use force to protect international peace and security.

Article I(2) expands on the use limitations of the first paragraph, stating that outer space shall be "free for exploration and use by all States without discrimination of any kind." This language affirms the principle of free access to space and prohibits interference with that access.[97] The language of paragraph two also contains an important condition that the use of outer space be "in accordance with international law." Thus, if the military action is otherwise lawful, the fact it is conducted in outer space or through information operations does not violate this provision.

Closely related to the freedom of access principle is the non-appropriation principle contained in Article II, which provides that outer space "is not subject to national appropriation by claim of sovereignty." While this language might suggest that information operations used to interfere with satellite signals or data are an act of unlawful appropriation of another State's space system, that view goes too far. Interference with a sovereign object is not the same as asserting a sovereign interest over outer space should that object be located there. Only the latter would violate the non-appropriation principle of Article II. The Law of the Sea Convention has similar language regarding claims over the high seas,[98] but it clearly has allowed use of the high seas by military warships (sovereign objects) without recognizing that interference with them constituted a claim of national appropriation over the high seas. Absent a claim of sovereignty over the high seas, interference with warships on the high seas has not been deemed equivalent to an unlawful appropriation. In both cases, what is prohibited is the assertion of territorial claims.[99]

Another potential limitation on information operations is contained in Article IV. This article contains the key provisions relating to military activity in space. Paragraph 1 prohibits nations from orbiting, installing on celestial bodies, or stationing in outer space any nuclear weapons or "any other weapons of mass destruction." The meaning of the term "weapons of mass destruction" (WMD) has "typically been defined as weapons that are intended to have indiscriminate effect upon large populations and large geographical areas."[100] It is generally accepted to include nuclear, chemical, and biological weapons.[101] Even though WMD could also include other weapons, notwithstanding the Russian position statement to the contrary,[102] the use of an information weapon is not likely to be viewed by the US as a weapon of mass destruction.[103] Ordinarily, its effects can be controlled so as not to destroy large numbers of people. For example, the

selective disabling by information operations of a particular computer system does not come within the meaning of WMD in Article IV.

For the most part, Article IV, paragraph 2, deals with the moon and other celestial bodies. Among other restrictions, it states that, "[t]he moon and other celestial bodies shall be used by all States Parties to the Treaty *exclusively for peaceful purposes*." It also states that "[t]he use of military personnel for scientific research or *for any other peaceful purposes* shall not be prohibited." Despite the fact that the "peaceful purposes" language does not expressly refer to the domain of outer space, historically the US and other nations have generally agreed that activities in outer space should also be confined to peaceful purposes.[104] Nonetheless, it has been the US view that the peaceful purpose language does not preclude lawful military activity.[105] While this conclusion seems clear, determining which military activities in outer space are considered "peaceful"[106] has been a topic of contentious debate. Indeed, from the moment the Outer Space Treaty was drafted, the international community has been divided on this issue.[107]

Advocates for the position that the "peaceful purposes" language excludes all military activity other than scientific research often cite to similar language in the Antarctic Treaty of 1959[108] and the conforming practice of nations in Antarctica. However, such a comparison is both misleading and inappropriate. Article 1, paragraph 1 of that treaty states that "Antarctica shall be used for peaceful purposes only." While this portion of the treaty is similar to the "exclusively for peaceful purposes" language of the Outer Space Treaty, the analysis is inapt. What many of these advocates fail to mention is *additional language* that is not found in the Outer Space Treaty. Immediately following the reference to "peaceful purposes," the text of the Antarctic Treaty states that "[t]here shall be prohibited, *inter alia,* any measures of a military nature . . . ." It is the additional language contained in the Antarctic Treaty, and not found in the Outer Space Treaty, that distinguishes the interpretation of the "peaceful purposes" language. Furthermore, State practice in Antarctica in 1959, when the treaty was drafted, was exclusively non-military while State practice in space in 1967, when the Outer Space Treaty was signed, was overwhelmingly military in nature.

The US view that Article IV does not preclude lawful military activity is also supported by the historical context in which the Outer Space Treaty came into existence. When the Outer Space Treaty was signed, its two primary drafters, the US and the Soviet Union, were already using outer space for military purposes. It is unlikely that the Outer Space Treaty was intended to proscribe existing practice by its two primary drafters.[109] The idea that "peaceful purposes" meant at least some military use was also consistent with the US space policy at the time. For instance, President Eisenhower declared to Congress, when the

National Aeronautical and Space Administration (NASA) was established, that the US was committed to the principle that "outer space be devoted to peaceful and scientific purposes."[110] Similarly, the Aeronautics and Space Act of 1958 contained language that "it is the policy of the United States that activities in space shall be devoted to peaceful purposes for the benefit of all mankind."[111] Despite use of such language, that same act provided for military departments to conduct space activities, including the development of weapons systems, military operations, and the defense of the US. Thus, the US has never interpreted "peaceful purposes" to mean only non-military activity. Rather, the US position has consistently been that the concept of "peaceful purposes" only prohibits aggressive military activity contrary to international law.[112] In 1962, Senator Albert Gore, Sr. stressed this distinction before the UN General Assembly. He urged that the "test of any space activities must not be whether it is military or non-military, but whether or not it is consistent with the UN Charter and other obligations of law."[113] While this view is not held by all,[114] it now appears to represent the international consensus[115] and is consistent with Article III of the treaty, discussed later. Therefore, any information operations undertaken in self-defense pursuant to a Security Council resolution, or in accordance with any recognized lawful purpose, would not be prohibited by either Article IV or other portions of the Outer Space Treaty. Moreover, during any period of international armed conflict, it is unlikely that these provisions would even apply between the belligerents who were parties to the treaty. While there are several views as to the test for when a treaty is abrogated or suspended by war between belligerent parties, the fundamental principle is the compatibility between the particular treaty provisions at issue and a state of war or armed conflict. Since the issue depends on the "intrinsic character" of the treaty provisions in question,[116] to the extent the Outer Space Treaty provisions being discussed here are incompatible with the object and purpose of armed conflict, they would most likely be suspended.

Finally, Article IX has the most direct application to the issue of information operations that interfere with the use of outer space by other nations. Indeed, the language of this article echoes principles enunciated earlier in the 1963 Declaration. In addition to requiring all States to conduct their activities in outer space "with due regard" for the interests of other States, it goes on to declare the following:

> If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, . . . would cause *potentially harmful interference* with activities of other States Parties in the peaceful exploration and use

> of outer space, . . . it shall undertake appropriate international consultations before proceeding with such activity. . . . (emphasis added)

Through this provision, the Outer Space Treaty made legally binding the 1963 Declaration's principle of prior consultation based on the potential for harmful interference in the space activities of another State.

Although the provisions cited above are likely to be interpreted in the international community to mean that "harmful interference" is prohibited, there are two important limitations to this prohibition as applied to information operations. The first is that the interference must be directed toward the "peaceful" use of space by other States. It is clear that a State may lawfully interfere with the space activities of other States when such activities are pursuant to a lawful use of military force. The second limitation is that the interference to the space system of another must be "harmful." Information operations that intrude upon, tap into, or monitor other space systems communications or other data for a military purpose can arguably be conducted without "harming" the space system of the other State, and to the extent they do no harm, they do not violate Article IX of the Outer Space Treaty.[117] Of course, regardless of such an argument, the State whose system was intruded upon would probably beg to differ. In fact, even if the intrusion were deemed not to violate Article IX, the political fallout could be extremely problematic.

Article III is perhaps the most important and illuminating of all the Outer Space Treaty provisions, the one which puts all the others into proper context. Article III states that the Parties "shall carry on activities in the exploration and use of outer space . . . *in accordance with international law, including the Charter of the United Nations,* in the interest of maintaining international peace and security . . . ." (emphasis added) It is this standard, far more than the oft-cited concept of peaceful purposes, that is central to whether or not activities in outer space comply with the Outer Space Treaty. While academic discussions will invariably center around the peaceful purposes language, military commanders, planners, and operators who are considering activities in outer space should focus instead on whether the military activity is lawful under the traditional law of armed conflict. If a nation's military activities are conducted "in accordance with international law" and the Charter of the UN, then the Outer Space Treaty recognizes that such activities can be in the interest of international peace and security. Consequently, it is Article III, not Article IV, that should be the primary focus of attention. Since the UN Charter is one of the standards cited in Article III, it is appropriate that we turn to that instrument.

2. UN Charter

Article 1 of the UN Charter expressly states that the purpose of the UN is to "maintain international peace and security." Accordingly, military activities aimed at restoring peace and conducted pursuant to a UN mandate or otherwise consistent with the Charter would be for a peaceful purpose. Article 39 of the Charter authorizes the Security Council to determine if a threat to peace, a breach of peace, or an act of aggression exists such that measures to restore international peace and security are required. Included among the lawful measures that the Security Council is authorized to direct in restoring peace and security are those set forth in Article 41, which include "the complete or partial interruption of... rail, sea, air, postal, telegraphic, radio, *and other means of communication*" (emphasis added). Clearly, information operations which have the effect of interrupting communications, and which are conducted pursuant to Article 41, would not only be lawful but an act undertaken to maintain or restore international peace and security. Therefore, such information operations would also be consistent with the Outer Space Treaty.

The UN Charter goes even further in allowing for military action to maintain or restore international peace and security. Article 42 authorizes "such action . . . as may be necessary to maintain or restore international peace and security" when Article 41 measures would be, or have proven to be, inadequate. By it, the Security Council has the authority to direct its members to "use all necessary means" to carry out Chapter VII peace enforcement measures, and, indeed, past resolutions such as Security Council Resolution 678 (DESERT STORM) in 1990[118] and Security Council Resolution 1264 (East Timor) in 1999[119] have contained this language. Coupled with the "all necessary means" language of a Security Council resolution, Article 42 allows information operations of far greater scope than merely interrupting communications, as authorized by Article 41. In determining the lawfulness of a particular information operation, it is necessary to evaluate the factual context, not just the type of information operation conducted.

Information operations can also be undertaken for purposes of individual or collective self-defense, an inherent right of all nations clearly recognized by Article 51 of the Charter. The mere fact that information operations affect space systems, or are conducted from outer space, does not make those operations illegal.

International Consortia and Other International Agreements

1. International Telecommunications Convention (ITC)

The ITC is the basic charter for the International Telecommunications Union (ITU), one of the oldest existing international organizations.[120] The ITU

directly oversees the communications satellite industry, arguably the most important sector of outer space activity.[121] A specialized agency of the United Nations since 1945,[122] it has been used by the UN to promote international cooperation in space[123] through the regulation of telecommunication services and allocation of radio frequencies.

Article 45(1) of the most recent ITU Convention, which was adopted in Geneva in 1992 and amended by the Plenipotentiary Conference at Kyoto in 1994, requires that all telecommunication stations operate so as not to cause "harmful interference" to the radio service or communications of other Members.[124] The convention defines "harmful interference" as "[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio-communication service operating in accordance with the Radio Regulations."[125] According to at least one scholar, the term is intended to be broadly interpreted and covers "any kind of damaging or destructive activity."[126] While this interpretation may have some academic value, it is not widely held, is not consistent with the express language of the ITC, and certainly does not represent the position of the United States.[127]

Information operations, such as implanting a trap door into the communications network of a potential adversary or setting up another type of then benign, but potentially destructive, cyber agent in the telecommunications system of another State, might be seen by some as "harmful interference." Arguably, because the purpose of its presence is to enable harmful interference or provide destructive capability when needed, the fact that an information operation mechanism is currently benign does not mean it is non-harmful. It would be difficult to show that this type of interference endangered the functioning of a service, seriously degraded it, or served to repeatedly interrupt it. However, even if there were found to be "harmful interference" from the activity, if the implanting of latent viruses or other cyber instruments were taken against a military network of another State, there would be no ITC violation. The ITC restrictions provide a recognized exception for "military radio installations" through Article 48(1). A more difficult situation arises when the activity affects a dual-use civilian telecommunication system, one used for both civilian and military purposes.

Finally, the ITC does not provide for its continued application between Party belligerents during armed conflict. Since its provisions are not compatible with the object and purpose of such hostilities, they will likely be considered suspended between the belligerents throughout the duration of any international armed conflict.[128] Thus, the only time the provisions in the ITC would apply

and possibly restrict some types of information operations would be when they do not rise to such a conflict level.

2. INTELSAT Agreement of 1973

Through the International Telecommunications Satellite Consortium (INTELSAT), the US initiated the first worldwide commercial telecommunications satellite system.[129] Created to encourage global nation-to-nation public satellite service,[130] INTELSAT reflects the US view of space law and policy. For example, within its basic structure, the consortium allows nations to invest and own shares in the organization, instead of it being organized along the old one-nation, one-vote concept. This voting and profit sharing formula reflects the US positions that space is to be used for the "benefit of mankind," and that the "province of mankind" does not require an equal apportioning of space wealth.[131] Despite these "American" views of space law, the Soviet Union joined INTELSAT in 1991;[132] there are currently 143 member countries. INTELSAT operates the world's most extensive global communications satellite system in existence, and DoD has been a user of the system from its advent.[133]

Articles III (d) and (e) of the INTELSAT Agreement describe military use of INTELSAT services. These provisions set forth a clear proscription on using "specialized telecommunications services" for military purposes. However, that proscription does not preclude INTELSAT from providing standard "public telecommunications services" to a military force for a military purpose.[134] In fact, according to a COMSAT legal opinion, aside from the limitation on using "specialized" services, "there is nothing in the INTELSAT Agreement that prohibits or discourages the use of INTELSAT for either US national security or intelligence purposes."[135]

The more difficult issue is the interruption, denial, or even destruction, of the data or data links from an INTELSAT system. There is nothing in the INTELSAT Agreement[136] that specifically prohibits interference with communication systems, although it certainly is implied throughout the agreement.[137] For example, Article XIV(d) of the agreement requires a party or signatory to consult with the Assembly of Parties and furnish all relevant information prior to using an INTELSAT space segment in a way that might prejudice the establishment of direct telecommunication links of other members.

INTELSAT's requirements of prior consultation and disclosure in advance of an operation would be completely unfeasible in the context of a military information operation. Absent some agreement with the members to the contrary, a Security Council resolution authorizing "all necessary means" under a

Chapter VII action, or some other lawful justification, this INTELSAT provision could serve to require disclosure and thus limit peacetime military information operations activities that interrupt, deny, or destroy another's data from an INTELSAT service. However, as with the other international agreements, during a period of international armed conflict, these limiting INTELSAT requirements will likely be viewed as suspended between the parties to the conflict, thus allowing jamming, destruction of ground stations belonging to an adversary, or other information operations.[138]

3. INMARSAT Convention

The International Maritime Satellite Organization (INMARSAT) was formed in 1976[139] to extend the INTELSAT framework to include maritime communications and certain maritime nations excluded from INTELSAT.[140] While its purpose was to provide space connections necessary to improve maritime and aeronautical communications, it has expanded into other systems, such as mobile communications.[141]

Article 3(3) of the INMARSAT Convention[142] provides that "the Organization shall act exclusively for peaceful purposes." Initially, INMARSAT took the view that military uses per se were not compatible with peaceful purposes unless they were for distress and safety or purposes recognized by international humanitarian law.[143] Much like the Outer Space Treaty, the INMARSAT Convention, in Article 12(1)(b), obligates the INMARSAT Assembly of Parties to ensure its activities are consistent with the UN Charter. INMARSAT's "peaceful purposes" language must therefore be read in the context of the UN Charter. When that is done, it becomes clear the INMARSAT Convention does not prohibit military action conducted under the auspices of the UN Security Council, legitimate individual or collective self-defense, or military action that is otherwise consistent with international law.

A recent privatization development, however, may have rendered the entire discussion over the meaning of "peaceful purposes" in the convention moot. On April 15, 1999, the assets and liabilities of the INMARSAT intergovernmental organization were transferred to a private company called, for lack of a better term, "new INMARSAT."[144] The new company's legal obligations arise out of its Memorandum of Association (MOA) and the Public Services Agreement (PSA) between it and the residual INMARSAT organization. The MOA requires new INMARSAT to "have due regard" for certain principles, including the "peaceful purposes" principle, but COMSAT's lawyers have taken the position that this language only requires the company to take those principles into consideration.[145]

Similarly, while clause 2.3 of the PSA provides that "[t]he Company shall act exclusively for peaceful purposes," the INMARSAT Assembly believed this language was political in nature and without an enforcement mechanism for alleged violations.[146] Therefore, according to the April 15, 1999, COMSAT General Counsel Opinion, "COMSAT envisions no circumstances in which the 'peaceful purposes' principle would be invoked as a reason to deny service to the US Department of Defense or units thereof."[147] That opinion, however, does not address whether "harmful interference" with a member's INMARSAT space segment or communication link would constitute a violation of its "peaceful purposes" language. Since the new organization is still based on the INMARSAT Agreement, it is not clear to what extent a member might seek to claim a violation of the provisions of that agreement. On the other hand, since new INMARSAT is now privatized, perhaps the only remedy to the private company shareholders would be contractual in nature. Regardless, potential disputes with offended nation shareholders will likely be avoided if the proposed military action is taken pursuant to the UN Charter or other international law.

4. Arms Reduction Treaties

Arms reduction treaties also contain provisions affecting the use of information operations. For instance, the ABM Treaty, in Article XII(2), was the first to preclude any activity which interfered with the "national technical means of verification" of treaty compliance by the other Party. Most other arms reduction treaties, such as SALT II and the START Treaty, have similar language.[148] While these formerly bilateral treaties are limited in the number of Parties involved, and there are concerns about what constitutes an unlawful interference with the national technical means of verification, the interference issue is certainly problematic. Although this matter merits further elaboration beyond the confines of this chapter, suffice it to say that information operations must be conducted so as to avoid interfering with national verification means during times other than international armed conflict.

5. Principles of the Law of Armed Conflict

Readily apparent in this overview of space law applicable to information operations is that despite all the sophisticated technology involved and the potential application of additional treaties and consortia agreements, by and large, the legal principles are the same as those applicable to other places and means of warfare. Just because military operations are planned for a unique domain—space—using a unique method—information operations—does not

change the fundamental legal constraints with which militaries must abide. It is imperative, as with all military actions, that a particular information operation in space or affecting a space object be conducted pursuant to a lawful purpose and in a lawful way. It is this second aspect of lawfulness that raises the issue of law of armed conflict (LOAC) principles. Notwithstanding the claims of some information operations supporters that this method of warfare transcends the scope of existing law, LOAC applies readily to information warfare techniques.[149]

Any offensive use of electronic means during military operations would implicate the traditional law of armed conflict principles. These include the counterbalancing principles of military necessity and the avoidance of superfluous injury, as well as the corollary principles of distinction of combatants from noncombatants, proportionality, and chivalry.[150]

The principle of military necessity is used to distinguish between what is and what is not a proper subject of attack.[151] It recognizes that enemy forces, along with their equipment, are always a proper subject of attack absent some other overriding LOAC principle. Similarly, civilians and civilian property that make a direct contribution to the war effort may be attacked, as long as their damage or destruction would produce a significant military advantage[152] or accomplish a legitimate military objective.[153] The presence of a dual-use system, commonly found in the arena of space systems, makes targeting analysis more difficult, but it does not change the fundamental analysis. Dual-use systems complicate the delineation of purely military targets from purely civilian non-targets. Therefore, targeteers must resist the temptation to attack a civilian computer system, such as a banking system, university, stock exchange, or similar target, merely because their attacks may have some vague effect on the enemy.

> 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.[154]

Accordingly, proposals to target civilian information systems must be examined closely to determine whether there is a military necessity for the attack. Other potential targets requiring close operational and legal analysis could include dual-use systems, such as navigation satellites or public communications systems, in which the data is provided through an international consortium such as INTELSAT, EUROSAT, or ARABSAT. Attacking data systems of international consortium organizations will likely affect many users of the data who are either not parties to the armed conflict or who are declared neutrals. Basically,

the target analysis will be the same when using information operations directed against space systems as it is using other means against other targets; it will just be more complex.

A complementary principle to military necessity is the avoidance of superfluous injury.[155] International law "forbids the infliction of suffering, injury or destruction not actually necessary for the accomplishment of legitimate military purposes. This principle of humanity results in a specific prohibition against unnecessary suffering [and] a requirement of proportionality."[156] It is the principle of superfluous injury that has led nations to agree to ban certain weapons.[157] In the context of information operations, it is difficult to imagine any specific use that has the potential of causing superfluous injury, but new technologies and uses require commanders to consider this principle.

Another important LOAC principle, distinction, demands that combatants be distinguished from noncombatants, and that military objectives be distinguished from protected property or places.[158] Only combatants and military objectives are to be attacked.[159] Additionally, indiscriminate attacks and methods and means of combat are also prohibited. A further aspect of this principle is that, with very limited exceptions, only members of a nation's regular armed forces are entitled to use force against the enemy.[160] To distinguish between combatants and noncombatants, the rule developed that combatants must wear a distinctive uniform.[161] In the case of an information operation initiated from a distant computer terminal, there is no practical need for the operator to be in uniform. However, this does not mean that the distinction between combatants and noncombatants during an information operation should not be retained.

> 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.[162]

The principle of proportionality requires that any civilian injury resulting from a legitimate use of military force not be disproportionate to the military advantages anticipated.[163] International law recognizes that attacks on lawful military targets can result in unavoidable collateral injury and damage to noncombatants and civilian property.[164] While the commander ordering the

attack is responsible for making this proportionality judgment, the defender has a responsibility to properly separate military targets from noncombatants and civilian property.[165] Information systems may be legitimate military targets, but an estimate of collateral damage and the damage from attacking them must take into account whether, and to what extent, they provide essential services to noncombatants.[166] This will require thorough intelligence information on an adversary's computer systems and networks to aid a decision that must be made on a case-by-case basis.

The final principle, chivalry, prohibits treachery or perfidy during armed conflict.[167] It demands a certain amount of fairness in offense and defense, as well as a certain mutual respect, honor, and trust between opposing forces.[168] When stratagems of war are developed, belligerents must be cautious not to subvert humanitarian safeguards to effect purely military goals.[169] For example, using a computer "morphing" technique to create an image of an enemy leader informing his military that an armistice or cease-fire agreement has been signed, when in fact no such agreement exists, would be an illegal perfidious act.[170]

Due to the complexity of applying LOAC principles to information operations against space systems, specific targeting proposals should be reviewed and approved in accordance with the rules of engagement in place and the procedures established by the National Command Authorities (NCA) or the Joint Force Commander, usually through a Joint Targeting Coordination Board.[171] Overall, information operations must be conducted consistent with the Standing Rules of Engagement (SROE) and may be used in individual or unit self-defense (as defined in the SROE) or with NCA approval.[172]

Application of General Law to Specific Scenarios

Having set forth the general legal framework applicable to information operations conducted in outer space or upon space systems, we now want to apply that framework to a series of escalating factual scenarios. While we hope these scenarios are somewhat realistic, they are not intended to imply that the United States or any other nation engages in such operations or even has the capability to do so.

Scenario 1: Implanting Sniffers and Trap Doors

Nation A has a security organization that obtains information from the Internet and attempts to gain information from other nations' computers. Nation A is especially concerned with the activities of Nation B, which has been

hostile in the past. Consequently, Nation A's security organization has directed covert activities toward Nation B. Both nations are industrialized and have well-developed infrastructures. Additionally, both nations have a space program that includes surveillance and telecommunications satellites with ground-based downlinks which provide data to the computers.

A security agent of Nation A reports to his supervisors that he has gained access, through the Internet, to the computer system that serves one of Nation B's unclassified military communications networks. This network uses space assets to ensure connectivity. He proposes implanting a trap door and "sniffer" that will, once in-place, remain inert and harmless, but which can be used to monitor data coming into this network.

Discussion

Obviously, gathering unclassified information readily available to the public is legal. However, implanting a trap door and "sniffer" which can be used to monitor space communication systems of another nation is more questionable. Most likely, such intrusions would violate the domestic laws of the offended State, but there is very little authority that, during peacetime, it would violate international law.[173] This type of information operation is likely to be viewed much as peacetime espionage is viewed, namely, of no significant concern unless serious practical consequences are shown.[174] As such, except for having to weather the diplomatic costs of protest and political rhetoric by Nation B, assuming they are able to ascribe the intrusion to Nation A, international law neither provides a remedy nor imposes any sanctions.

Specific space law provisions similarly provide no legal restraint on this intrusion. The Outer Space Treaty only applies to activities in outer space, the moon, and other celestial bodies and is, therefore, not applicable to an intrusion into a ground system. Assuming Nation B is an ITU member and the system intruded is a system regulated by the ITU, then some might suggest that the ITC applies. They would be in error. As noted above, Article 45(1) of the ITC prohibits "harmful interference"—that which "endangers the functioning" of a radionavigation service or "degrades, obstructs or repeatedly interrupts" a radio communication service. Trap doors and "sniffers" do not degrade, obstruct, or interrupt communications. Moreover, such a cyber intrusion arguably does not "endanger the functioning" of the communication service.

Likewise, such an act would not violate the UN Charter. Implanting a monitoring device that establishes a passageway for future intrusions is all that this information operation entails. Such implanting is akin to a covert intrusion into the command and control center of another country and placing a monitoring

device on the phones. This action would neither endanger international peace and security under Article 2(3) of the UN Charter, nor would it constitute a threat to the political independence of any State under Article 2(4). While this type of computer penetration might constitute a threat to the territorial integrity of a UN member State, it will likely be treated much like espionage, which State practice has clearly accepted, at least tacitly. As such, it can be accomplished with little risk of prosecution under international law or UN sanction. The fact this particular intelligence gathering activity is conducted using information operations that impacts data from a space system, rather than more traditional means of espionage, does not change the basic equation.

In sum, this first scenario does not present any legal obstacles or limitations under either space law or international law. Nonetheless, it could be highly volatile in the political arena and would present a delicate policy decision that must be made by the NCA.

Scenario 2: Interruption of Command and Control Networks

Tensions between A and B increase, but have not risen to the level of armed conflict. At this point, another security agent from Nation A gains access to one of B's unclassified military communications networks through the trap door previously implanted. He temporarily jams the network so that contact with B's orbiting satellites will be interrupted for a period of approximately 30 minutes. After about twenty minutes, Nation B's space technicians regain control of their satellite network and restore normal communications. There is no damage to the satellite or permanent disruption of its functions.

Discussion

Since this has not occurred during an armed conflict, some might argue that interfering with the satellite network of Nation B would constitute a violation of Article 45(1) of the ITC if the 20-minute interruption of communications is deemed to be "harmful interference." The ITC definition requires that the interference endanger the functioning of a radionavigation service or other safety service, or seriously degrade, obstruct, or repeatedly interrupt a radio- communication service. Whether or not a 20-minute interruption of satellite communication constitutes a serious degradation or obstruction might depend on the precise nature of the communications that were interrupted. For instance, if critical search and rescue systems were interrupted thereby resulting in the loss of life of Nation B citizens, then perhaps the interruption would be seen as harmful, even though the space system itself may not have been damaged or harmed.

Under the UN Charter, there is some legal basis for the proposition that taking control of another nation's communications system or space assets may interfere in the internal affairs of that nation thus violating its rights under the UN Charter. This would be especially true if the interruption resulted in loss of life as noted above. It might also be true if the space system interrupted was particularly important to Nation B's defense, such as a missile early warning system. Any determination that rights under the UN Charter were violated or not will depend, as it will under the ITC, on the precise nature of the system that is interrupted. In this scenario, Nation A's interruption of one of Nation B's unclassified communication systems was temporary and it did not detract from sensitive military systems. Absent at least resulting moderate damage or injury, an armed response in self-defense by Nation B would not appear to be justified. Most likely, the primary costs of this scenario would be political in nature.

Scenario 3: Moving an Adversary's Satellite Out of Effective Orbit

Nation A knows that Nation B has a military reconnaissance satellite with high resolution capability that can provide Nation B with critical intelligence on the movements of Nation A's troops. Nation A is concerned about recent bellicose statements made by Nation B toward Nation A and wants to mobilize several thousand troops along their shared border. In anticipation of the outbreak of armed conflict, Nation A covertly obtains internal access to B's classified military computer system and uses information operations to send false data instructions to the Nation B satellite. While this false data does not damage the satellite, it does cause the satellite to move into another orbit where its surveillance capabilities are rendered completely ineffective.

Discussion

As in the prior two scenarios, there is no physical damage or destruction involved with the satellite or systems of Nation B and armed conflict has not yet arisen. Unlike Scenario 2 though, this interference with Nation B's military satellite will require Nation B to take steps to "recover" the satellite and restore its prior orbit before it can be effective. In effect, the satellite has been "kidnapped" at a militarily critical point, providing Nation A with a distinct military advantage should armed conflict occur.

Since this scenario involves a military satellite and not an INTELSAT system or asset, the INTELSAT Agreement does not apply. Therefore, there is no requirement under Article XIV(d) of the INTELSAT Agreement of prior consultation or to provide all relevant data regarding the interference. Furthermore, as

long as the satellite was not engaged in conducting Nation B's "national technical means of verification" of arms control obligations, the interference would not violate the ABM Treaty or similar arms control treaty verification provisions,[175] assuming A and B were Parties.

The problem raised in this scenario derives again from the UN Charter. Assuming Nation B's satellite is considered part of Nation B's "sovereignty" or "territorial integrity," Nation A's actions to involuntarily move it out of orbit could be viewed as a "threat . . . against the territorial integrity or political independence of any state" in violation of Article 2(4). If so, the Security Council, under Article 39, would be authorized to decide what appropriate measures to take against Nation A to restore international peace and security. Given the national security importance of this reconnaissance satellite to early warning, the Security Council might determine that this act rises to the level of an "armed attack" sufficient for Nation B to invoke its right of self-defense under Article 51 of the UN Charter. In addition, Nation B might determine independently that the action requires it to invoke its inherent right of self-defense without waiting for a UN determination.

Scenario 4: Destruction of Adversary's Satellite

As anticipated, armed conflict has now broken out between Nations A and B. Nation A's troops, previously amassed along Nation B's border and heavily armed, have crossed into Nation B. Numerous reports indicate Nation A's troops have been firing at Nation B's military forces as they approach the nearest town. An emergency session of the Security Council has been called to address the situation, but no UN response has yet been authorized. Moreover, since Nation A is a close ally of a permanent member of the Security Council, a veto of any UN action against it is anticipated. Nation B's targeteers propose to destroy a key hub in the space communications system of Nation A and render its connected computers useless. They plan to maneuver one of their own satellites within close range of one of Nation A's telecommunications satellite. This "killer" satellite has been equipped with a device that, when activated, will emit an electro-magnetic pulse which will disable all electronic devices within a ten-mile radius. Destruction of the targeted satellite, located in geosynchronous orbit over the area of armed conflict, will render Nation A's entire communication system inoperable.

Discussion

This scenario presents a clear armed conflict situation that very likely renders the Outer Space Treaty, the ITC, and any arms control agreements

inapplicable.[176] If there is any doubt as to whether these international agreements were intended to be suspended or terminated during armed conflict, Nation B could make a prior declaration that it considers each of them inapplicable during this period of armed conflict with Nation A.

Nation B could choose, for policy reasons, to treat this as an "armed attack" and exercise its right of individual self-defense, or it could treat A's incursion as "an act of aggression" under Article 39 of the UN Charter and seek Chapter VII sanctions through the UN. Before Nation B can exercise its right of self-defense through use of force, Article 33 of the UN Charter requires it to exhaust any available peaceful means of settlement, unless, of course, such efforts would be futile.[177] Seeking action through the Security Council would likely prove fruitless, since Nation A is a close ally of a permanent member with veto authority. Regardless, Nation B's armed response must be necessary, timely, and proportionate to the wrong suffered.[178]

Given the military value to Nation A of this satellite system, there would be a legitimate military necessity in attacking this space asset. Destruction of Nation A's satellite would put the military aggressors at a distinct disadvantage in obtaining and disseminating intelligence and communication data without resulting in loss of life. Additionally, since the targeted space communications system is used for military communications, even though it also has a civilian use, there is a legitimate military reason to attack it. The principle of proportionality requires Nation B's commanders to make their best estimate of the military advantage to be gained and weigh it against their best estimate of the effect on the civilian population. The extent of injury or damage to the civilian population from interruption of a communication system through information operations is likely to be significantly less than from kinetic weapons. Additionally, this particular information operation, used as a weapon, is neither illegal *per se* under international law, nor are its effects necessarily indiscriminate. Indiscriminate weapons are those whose effects cannot be controlled, such as chemical and biological weapons. The wide area in which this weapon's effects will be felt do not make it indiscriminate, especially since its effects will be short-term, and limited to disabling electronic devices.

Readily apparent from each of these scenarios is the importance of making a case-by-case assessment under international law, and more particularly, LOAC principles. As with any LOAC assessment, a proper determination of a specific information operation can only be obtained by applying the specific facts to the general legal framework. What makes the assessments of information operations directed at or from space systems more difficult is the lack of extensive State practice to rely on.

Practical Considerations in the Application of Information Operations in Space

In addition to the legal regime applicable to information operations in outer space, military planners should also factor the unique physical aspects of space and the political consequences of specific military decisions into their calculations. In this final section, we have attempted to set forth a few such considerations. Keep in mind however, that they are not based on legal constraints, but rather on the physical properties of outer space and the political climate of the international community. Additionally, these considerations are not intended to preclude a commander's discretion as to the appropriate military action to be taken given the specific military situation faced.

First, any attack upon a physical target in space should seek to disable the space object without resorting to its physical destruction. Absent the effects of gravity and friction, fragments from physical destruction of space objects present a significant problem in outer space. Those fragments will naturally spread throughout the orbital path they came from in an unavoidable pattern that may not dissipate. Their velocity and mass will make them a threat to our own space vehicles and satellites. Confining the effects of that debris will be difficult, if not impossible. Certain information operations in space can provide an alternative to the military planner to outright physical destruction of an adversary's space object by destroying the computer links and data (its life support). Thus, "killing" of the object may be possible without creating a dangerous spread of fragments to our own space systems.

Second, if a space system needs to be destroyed, consideration should be given to destroying it by attacking its ground segment, and thereby severing access to its "life support." Attacks on ground segments of communications systems have received long-standing public acceptance in the international community as an authorized means of conducting armed conflict as long as the target is a legitimate military target. A direct attack on a space segment in space, even if done consistent with international law, may not enjoy the same public acceptance. Given the importance of international opinion upon national leaders and their citizens, military action often attempts to avoid undue public outcry in making target selections. Therefore, if there is a choice, it may be better to take out an adversary's space object by attacking and destroying its ground segment.

Third, destruction through "jamming" of a communication signal is preferable to destruction of the adversary's space object and accomplishes the same result—the enemy's inability to use that system. Just as ground attacks have received public acceptance, so too has the technique of jamming. It is a common practice during

armed conflict and is clearly recognized as a legitimate means of attack. As such, and for reasons of avoiding undue public outcry, jamming should be considered as an alternative to the outright physical destruction of the space object. Additionally, jamming avoids the problem of unnecessary space debris.

Fourth, a less intrusive electronic means of attack is often preferable to a kinetic kill. Electronic attack can be a better means of avoiding detection while "masking" the identity of the perpetrator. When subtlety or plausible denial is desired for political reasons, or if there is a need to delay enemy detection of the attack, electronic means can be very effective. When an adversary's system goes down, they will not necessarily know it was the result of an intentional act by an enemy. This is especially so if the system is left operable, but has been manipulated so that the system data is, or appears to be, false. Depending on the system attacked, this manipulation can cause military planes to crash, artillery to miss its target, or enemy leaders to make poor decisions.

No doubt, many other practical approaches to the use of information operations in outer space or directed toward space objects have not been mentioned here. Those offered are but a limited start for planners and strategists when considering the unique aspects of these two technologically driven realms (information operations and outer space) during armed conflict.

Conclusion

We began this chapter with the observation that when the technological transformations inherent in outer space systems are combined with that of information operations, yesterday's science fiction can quickly become today's reality. The need for militaries to keep pace is obvious. These technological transformations will require innovative approaches to an ancient reality—armed conflict between belligerent nations. Information operations and modern space systems have created new warfighting scenarios that can, in turn, create confusion among military commanders and planners as to what is lawful and what is not. It is imperative that operators and lawyers forge a partnership to meet this challenge.

As for what is legal in the outer space environment, there are few surprises. Still relevant is traditional analysis under well-known principles of the law of armed conflict, customary international law, treaty obligations, and the UN Charter. Aside from the need to apply the existing analytical framework to new futuristic threats, there are few legal limitations impacting information operations in or through outer space.

The real challenge comes in understanding the expansion of international *political* sensitivities to weapons in space and information operations directed at or

from outer space. During times of armed conflict, those sensitivities will not create violations of international law, but they can impede our actions through the political and diplomatic process. We should not underestimate the degree to which politics and diplomacy place limits upon otherwise lawful military activity. Thus, with only a few exceptions, from a legal standpoint, information operations in space are virtually no different than those conducted on the ground, in the air, or at sea. The primary difference lies in the diplomatic and political response of the international community.

Moreover, the "CNN factor" has had a large role to play in the decisions of military commanders to employ ground, sea, and air assets in recent armed conflicts. We can expect the influence of the "CNN factor" to grow exponentially if military commanders choose to employ information operations against objects in outer space, a much more sensitive arena. Indeed, because of this, commanders may find their authority to choose targets and the means of attacking those targets withheld by the NCA in this arena more than any other.

All that aside, however, once the political decision has been made, commanders should apply the same principles of international law they do in more conventional settings. They must avoid the dizzying distraction created by the vast array of new technological tools available to the military in the space arena; they must resist the temptation of expecting that these apparent futuristic tools require a whole new set of laws; and they must be willing to apply old laws and principles to new military scenarios. If they can do that, then tomorrow's commanders can maintain the *legal* high ground of warfare, while controlling the *military* high ground of outer space. This is not a matter of science fiction; it is reality.

Notes

* The authors would like to thank the following people for their assistance in reviewing this chapter: Mr. Phillip Johnson (Colonel, USAF, (ret.)), Mr. Michael Schlabs (Colonel, USAF (ret.)), Colonel Kevin Kennedy, (USAF), Lieutenant Colonel Mark Yost (USAFR), Lieutenant Colonel Jolinder Dhillon (USAF), Lieutenant Colonel Jeff Walker (USAF), and Lieutenant Colonel Jeff Rockwell (USAF).

1. Nathaniel Borenstein, quoted from *Zeebo's Marvelous Quotes, Quotes about Computers* (Sept. 3, 2000) http://quotes.sterlingtechnology.com/key/key_Computers.html.

2. For instance, military parades of the future could be comprised of rank after impressive rank of glistening computer terminals passing in review instead of shiny tanks and rifle-carrying soldiers; the sides of military computers of the future may be painted with rows of mean looking Internet wires to represent each "kill" of tomorrow's computer aces; and recruiting posters may have a picture of a computer geek with lines of pencils sticking out of his pocket protector and a caption beneath saying, "We want you!" While these scenarios are a bit far-fetched, there is no denying the importance of computers in the battles of the future.

3. *Pentagon Officials Warn of Electronic Pearl Harbor*, MILITARY & C4I, March 11, 1999, at n.p.

4. Charlie Williamson, *Emerging Issues in Cyberdefense,* ABA NATIONAL SECURITY LAW REPORT, Aug. 1999, at 2; A REPORT OF THE PRESIDENT OF THE UNITED STATES, PRESERVING AMERICA'S PRIVACY AND SECURITY IN THE NEXT CENTURY: A STRATEGY FOR AMERICA IN CYBERSPACE, Sept. 16, 1999, at 6 [hereinafter referred to as REPORT OF THE PRESIDENT].

5. This rate of detection represents those that are reported. *See* Ted Uchida, School of Advanced Military Studies, US Army Command and General Staff College, Building a Basis for Information Warfare Rules of Engagement 8 (1997) (unpublished manuscript, on file with Naval War College Library), *cited in* 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, 893 (1999).

6. The intruding teenage hackers were from California and aided by an Israeli teenager acting as their advisor. They were able to exploit a well-known weakness in an operator system called "Solaris." USIS Washington File, *On Information Warfare Threat,* MILITARY & C4I, Infowar.com, Dec. 14, 1998; *See also* Bradley Graham, *U.S. Studies New Threat: Cyber Attack,* WASHINGTON POST, May 24, 1998 at A1; WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 20 (1999); E. Anders Ericksson, *Information Warfare: Hype or Reality?* 6 THE NONPROLIFERATION REVIEW, n.13 (1999).

7. MILITARY AND C4I, *supra* note 3, at 3.

8. SHARP, *supra* note 6, at 19.

9. Schmitt, *supra* note 5, at 887.

10. Bob Brewin, *Kosovo Ushered in Cyberwar,* FEDERAL COMPUTER WEEK, Sept. 27, 1999, at 1.

11. White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 1998).

12. Kevin Poulsen, *Info War or Electronic Saber Rattling?,* ZDNN TECH NEWS NOW, (Sept. 8, 1999), at 1–2.

13. *Id.* The JTF-CND Commander reports to the SECDEF through the Chairman of the Joint Chiefs of Staff. The Commander "has directive authority over assigned forces designated by Service components for execution of the CND mission, and coordinates with and supports commanders of combatant commands." Williamson, *supra* note 4, at 2.

14. USAF SCIENTIFIC ADVISORY BOARD, NEW WORLD VISTAS, AIR AND SPACE POWER FOR THE 21ST CENTURY (Information Applications Volume), at 3 (1995).

15. *Id.* A presence in space implies influence, power, and security.

16. *Id.* at 4.

17. Michael Loescher, *The Information Warfare Campaign, in* ALAN D. CAMPEN, DOUGLAS H. DEARTH & R. THOMAS GOODDEN, CYBERWAR 197 (1996).

18. REPORT OF THE PRESIDENT, *supra* note 4.

19. *See* Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and "Peaceful Purposes,"* 60 JOURNAL OF AIR LAW AND COMMERCE 237, 248 (1994); SEAN P. KANUCK, *Recent Development: Information Warfare: New Challenges for Public International Law,* 37 HARVARD INTERNATIONAL LAW JOURNAL 272, 285 (1996).

20. GERALD R. HUST, TAKING DOWN TELECOMMUNICATIONS 4 (1994).

21. *Id.*

22. Of particular application is 18 USCode 1367, a federal criminal statute that prohibits the intentional or malicious interference with the authorized operation of a communications or weather satellite without the authority of the satellite operator. Also potentially applicable, in addition to US wiretap laws and depending on where the cyber attack originates, is 18 US Code 1030, which prohibits damaging protected computers by inserting viruses or other technological items; 47 US Code 333, which prohibits interference with licensed radio stations; and 47 US Code 502, which prohibits violation of international radio or communications treaties.

23. Air Force Doctrine Document (AFDD) 2-5, Information Operations, Aug. 5, 1998. As an example of the different terms used by the various military services, and as noted in the text, the Air Force is the only service to employ the term "information-in-warfare."

24. *Id.* Likewise, the Air Force definition of "information warfare" differs from that of DoD. For the Air Force, information warfare is a subcategory of information operations that is not confined to armed conflict. In contrast, the DoD sees "information warfare" as information operations "conducted during times of crisis or conflict." *Id.*, glossary.

25. John Deutsch, Testimony before the Senate Committee on Government Affairs (June 5, 1996).

26. JOHN ARQUILLA & DAVID RONFELDT, CYBERWAR IS COMING, RAND (1992).

27. Headquarters Air Force, International and Operations Law Division, Primer on Legal Issues in Information Operations, (draft), at 3 (1997). The term "offensive information operations" is intended to apply to the entire spectrum of military operations throughout peacetime through armed conflict, including military operations other than war. Offensive information operations embrace a great variety of activities, including psychological operations, military deception, jamming of enemy information systems, signals intelligence (SIGINT), and attacks on enemy information systems by physical destruction or by electronic means.

28. "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles." ARQUILLA, *supra* note 26, at 6.

29. *Id.* at 5.

30. Daniel Kuehl, What's New about Information Warfare?, at 10 (March 21, 1997), (unpublished NDU paper), cited in YuLin G. Whitehead, Information as a Weapon, Reality versus Promises 19 (January 1999), (unpublished School of Advanced Airpower Studies paper, Air University).

31. Interview by YuLin Whitehead with Daniel Kuehl, National Defense University, *cited in* Whitehead, *supra* note 31, at 19.

32. Joint Publication 3-13, II-9; Air Force Doctrine Document 2-5, Information Operations, at 9 (Aug. 5, 98); Air Force Doctrine Document 2-2, Space Operations, at 8 (Aug. 23, 1998). Winning the battle of information dominance requires that we achieve an edge in offensive exploitation of the enemy's vulnerabilities over its ability to penetrate our protective measures.

33. MAO TSE-TUNG, ON PROTRACTED WAR (1938), *cited in* NORMAN B. HUTCHERSON, COMMAND AND CONTROL WARFARE, PUTTING ANOTHER TOOL IN THE WAR-FIGHTER'S DATA BASE, at xiii (1994).

34. *See* HUTCHERSON, *supra* note 33, at xiii.

35. *See generally*, Department of Defense Space Policy contained in DoD Directive 3100.10, paragraph 4, specifically sub-paragraphs 4.3.1.4 and 4.3.1.7.

36. COLIN S. GRAY, EXPLORATIONS IN STRATEGY 102 (1996); *see also* Colin S. Gray and John B. Sheldon, *Space Power and the Revolution in Military Affairs*, AIRPOWER JOURNAL, Fall 1999, at 32.

37. Gray and Sheldon, supra note 36, at 32.

38. *Control of Space Key to Future War*, SPACE DAILY, May 10, 1999, at 1. There is also a political advantage to space forces over conventional forces. With conventional forces, policy makers have to contend with the possible loss of troops' lives when deploying them into battle. Use of space forces does not have that disadvantage. Major General DeKok, Air Force Space Command's Director of Operations and Plans, captured the difference when he remarked that, "Satellites have no mothers." Gregory Billman, *The Inherent Limitations of Spacepower: Fact or Fiction?* E-PRINTS, Sept. 22, 1999, at 21, www.fas.org/spp/eprint/billman.htm.

39. *Id.*

40. *Id.* The basic GPS consists of a constellation of 24 satellites, their navigation payloads, and associated ground stations, data links, and command and control facilities, and is operated by the DoD. It has become an integral part of US military operations.

41. The White House Fact Sheet, National Space Policy, Sept 19, 1996 at 1 [hereinafter Space Policy].

42. The following countries have communications satellites in orbit: Argentina, Australia, Brazil, Canada, China, Cuba, Finland, France, India, Indonesia, Italy, Japan, Malaysia, Malta, Mexico, New Guinea, Russia, Seychelles, Spain, Tonga, United Kingdom, and the US. Several other nations have access through cooperative agreements, such as the Association of Telecommunications State Enterprises of the Sub-Regional Andean Agreement (ASETA), comprised of Bolivia, Colombia, Ecuador, Peru, and Venezuela. *See* Morgan, *supra* note 19, at 247–248.

43. T. S. Twibell, *Note and Comment: Circumnavigating International Space Law*, 4 ILSA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW, 259, 276 (Fall, 1997). In fact, as of November 21, 1999, China had successfully launched into orbit its first spacecraft designed to carry humans in an effort to join the US and Russia in the elite club of manned space flight. The unmanned module orbited the earth 14 times before it parachuted into a field in Inner Mongolia, 21 hours after taking off. Michael Laris, *China Launches New Spacecraft Designed for Manned Flight*, WASHINGTON POST, Nov. 22, 1999, at A1 .

44. Gerald Steinberg, *Dual Use Aspects of Commercial High-Resolution Imaging Satellites*, MIDEAST SECURITY AND POLICY STUDIES, Feb. 1998, at 3.

45. The latest of the SPOT imaging satellites, SPOT-4, has a 10 meter monochromatic resolution as well as an additional mid-infrared imaging capability. The French are presently working on SPOT-5A and 5B which they hope to launch in 2000 and 2003. *See* Steinberg, *supra* note 44, at 3. Satellites are now available to provide detailed images of any requested location in the world once every three days at a cost of as little as $100 per square mile. *See* Susan M. Jackson, *Cultural Lag and the International Law of Remote Sensing*, 23 BROOKLYN JOURNAL OF INTERNATIONAL LAW 853, 854 (1998).

46. Jackson, *supra* note 45, at 857.

47. *Id.* at 858.

48. On March 29, 1996, President Clinton announced a new policy to terminate the practice of degrading civil GPS signals within the next decade, allowing for a better signal for commercial and civilian users of the GPS. The policy expressly states that it is meant to reaffirm the US commitment to providing basic GPS services for peaceful civil, commercial, and scientific users. Press Release, President Opens Door to Commercial GPS Markets; Move Could Add 100,000 New Jobs to Economy by Year 2000, March 29, 1996.

49. Lane, The Satellite Revolution, *cited in* Steinberg, *supra* note 44, at 16.

50. G.A. Res. 1148, 12 U.N. GAOR Supp. (No. 18), at 195, U.N. Doc. A/3805 (1957), para. 1(f) ("the sending of objects through outer space shall be exclusively for peaceful and scientific purposes"); G.A. Res. 1348, 13 U.N. GAOR Supp. (No. 18), at 99, U.N. Doc. A/4090 (1958) ("outer space should be used for peaceful purposes only . . . .").

51. The words of a former Commander-in-Chief of USSPACECOM, General Howell M. Estes, are indicative of this view:

> I, as a military commander, have to say that somebody is going to threaten them (our space assets); and when they [do], we [should] have armed forces to protect them. . . . [I]f there was ever a threat to our national security [in space], the best—and only— way to solve the problem is to take weapons into space.

Cited in Jose Filho, *Total Militarization of Space and Space Law: The Future of Article IV of the '67 Outer Space Treaty*, PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 358, 360 (1997).

52. G.A. Res. 1472 (Dec.12, 1959). Actually, COPUOS began as an Ad Hoc Committee on September 18, 1958. Its first report, adopted as Resolution 1348 on December 13, 1958, stressed that outer space should be used only for peaceful purposes. The next year, General Assembly Resolution 1472 made the Ad Hoc Committee a permanent UN committee.

53. Those four treaties are: (1) The Treaty on Principles Governing the Activities of States in the Exploration and Uses of Outer Space, including the Moon and Other Celestial Bodies (known as the Outer Space Treaty of 1967), *done* Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347; 610 U.N.T.S. 205, (*entered into force* Oct. 10, 1967); (2) Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (known as the Rescue and Return Treaty of 1968), *done* Apr. 22, 1968, 19 U.S.T. 7570, T.I.A.S. No. 6599, 672 U.N.T.S. 119, (*entered into force* Dec. 3, 1968); (3) The Convention on International Liability for Damage Caused by Space Objects (known as The Liability Convention of 1972), *done* Mar. 29, 1972, 24 U.S.T. 2389, T.I.A.S. No. 7762, 961 U.N.T.S. 187 (*entered into force* Sept. 1, 1972); and (4) The Convention on Registration of Objects Launched into Outer Space (known as The Registration Convention of 1975), *opened for signature* Jan. 14, 1975, 28 U.S.T. 695, T.I.A.S. No. 8480, 1023 U.N.T.S. 15 (*entered into force* Sept. 15, 1979). A fifth UN sponsored space treaty is The Treaty Governing the Activities of States on the Moon and Other Celestial Bodies (known as The Moon Treaty of 1979). It has only been ratified by 9 nations and none of the major space powers.

54. G.A. Res. 1721, U.N. Doc. A/5100 (1961). *See also* John E. Parkerson, Jr., *International Legal Implications of the Strategic Defense Initiative*, 116 MILITARY LAW REVIEW 67, 95 (1987).

55. U.N. Doc. A/5515 (1963).

56. The Committee has two standing Subcommittees of the Whole: the Scientific and Technical Subcommittee and the Legal Subcommittee. The Committee and two Subcommittees meet each year to discuss and study questions put to them by the General Assembly. They in turn make recommendations to the General Assembly and provide information from their meetings and studies in their annual reports. *See* the COPUOS web page at www.un.or.at/OOSA/copuos.html.

57. G.A. Res. 51/44 (Jan. 7, 1997).

58. *See* G.A. Res. 53/583 (Dec. 4,1998); G.A. Res. 52/56 (Feb. 12, 1998); G.A. Res. 51/123 (Feb. 10, 1997); G.A. Res. 51/122 (Feb. 4, 1997); and G.A. Res. 49/34 (Jan. 30, 1995). Also of interest is what these resolutions do not address: namely, the important contribution of military activity toward promoting international peace and security, such as reconnaissance satellite data that allows for the more effective verification of arms control agreements.

59. NATHAN C. GOLDMAN, AMERICAN SPACE LAW: INTERNATIONAL AND DOMESTIC 26 (2d ed. 1996). Goldman also notes that more nations became aware of the values of space and sought to join the committee to protect their interests. COPUOS tripled in size in 1982, from 18 members to 53. According to Goldman, the "drastic increase in size alone would guarantee a harder time for obtaining consensus."

60. *Id.* at 25.

61. The UN Charter does not grant the General Assembly legal authority to make binding substantive international law. *See* Andrei D. Terekhov, *UN General Assembly Resolutions and Outer Space Law*, PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 97 (1997).

62. The following principles derived from the four major space treaties have also been generally accepted as reflecting customary international law:

(1) That outer space is free for exploration and use by all nations; that it is not subject to national appropriation by any means;

(2) That activities in outer space shall be conducted with due regard for the interests of other States;

(3) That 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. That there are two liability standards established for damage caused by "space objects;" a fault-based standard that applies to damage done to items in space and an absolute liability standard that applies to damage done on the surface of the earth or to aircraft in flight; and

(4) Outer space activities are subject to general principles of international law, including the UN Charter.

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

63. *See* Terekhov, *supra* note 61.

64. *See* the Conference on Disarmament web page at www.unog.ch/frames/disarm/disconf.htm.

65. P.K. MENON, THE UNITED NATIONS' EFFORTS TO OUTLAW THE ARMS RACE IN OUTER SPACE 65 (1988).

66. *Id.*

67. *Id.* at 66.

68. *Id.*

69. Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, *signed on* May 26, 1972, 23 U.S.T. 3435, 944 U.N.T.S. 13, TIAS 7503 (*ratified by the US on* Sept. 30, 1972); Rebecca Johnson, *Multilateral Arms Control: Can the CD Break the Impasse?*, www.armscontrol.org/ACT/novdec97/johnson.htm.

70. *See* Johnson, *supra* note 69, at 6.

71. *See* DoD/GC Paper, *supra* note 62.

72. China Defense White Paper, July 1998, http://russia.shaps.hawaii.edu/security/ china-defense-july1998.html (on file with authors).

73. *Id.* at 24.

74. *Id.*

75. In an article published in the *Liberation Army Daily*, official Chinese newspaper of the Communist Party-run political department of the Peoples Liberation Army (PLA), entitled "Bringing Internet Warfare Into the Military System Is of Equal Significance with Land, Sea, and Air Power," China seems to have changed its view about the use of information operations. According to the Beijing article, China is preparing to "carry out high-technology warfare over the Internet and could develop a fourth branch of the armed services devoted to information warfare." The article also stated:

> It is essential to have an all-conquering offensive technology and to develop software and technology for Net offensives so as to be able to launch attacks and countermeasures on the Net, including information-paralyzing software, information-blocking software, and information-deception software.

The article went on to apply this new means of warfare to outer space:

> Modern high-tech warfare cannot win without the Net, nor can it be won just on the Net. In the future there must be a coordinated land, sea, air, *space*, electronic and Net warfare, and the state's determination will be fully expressed in this mysterious theater space (emphasis added).

Quoted in Bill Gertz, *China Plots Winning Role in Cyberspace*, THE WASHINGTON TIMES, Nov. 17, 1999, at A1, A8.

76. Agenda item number 3, Report of the Conference on Disarmament to the General Assembly of the United Nations, at 2 (Sept. 8, 1998).

77. CD/1487, Working Paper Concerning CD Action on Outer Space (Jan. 21, 1998).

78. *Id.*

79. Space Policy, *supra* note 41, at 4 (Sept.19, 1996).

80. *See* Filho, *supra* note 51, at 358; *see also* Maurice N. Andem, *Implementation of Article IV of the Outer Space Treaty of 1967 During the 21st Century,* PROCEEDINGS OF THE FORTIETH COLLOQUIUM ON THE LAW OF OUTER SPACE 338 (1997).

81. Space Policy, *supra* note 41, at 1.

82. *Id.* at 5, para. (6)(b).

83. *Id.* at 5, para. (6)(a).

84. DoD Directive 3100.10, paragraph 4.3., states that "[t]he primary DoD goal for space and space-related activities is to provide operational space force capabilities to ensure that the United States has the space power to achieve its national security objectives . . . ." That includes assuring access to space (para. 4.3.1.2.) and ensuring that hostile forces cannot prevent our use of space (para. 4.3.1.4.).

85. Memorandum for Secretaries of the Military Departments, July 9, 1999, at 2 (on file with authors).

86. In September 1994, former Secretary of the Air Force Sheila Widnall stated, "Certainly, part of the Air Force mission is control of space, our ability to deny the use of space if necessary." Filho, *supra* note 51, at 359; General Joseph W. Ashy, former Commander-in-Chief of USSPACECOM, declared in 1996; "We are going to fight in space. Some people don't want to hear this, and it isn't in vogue. . . but – absolutely – we are going to fight in space." *Id.*

87. DoD Directive 3100.10, *supra* note 84, at para. 4.1.

88. Prohibited military activities in outer space that are specified in multilateral agreements include the following:

(1) placing nuclear weapons in earth orbit, on celestial bodies, or anywhere else in outer space (Article IV, paragraph 1, Outer Space Treaty);

(2) placing weapons of mass destruction in earth orbit, on celestial bodies, or anywhere in outer space (Article IV, paragraph 1, Outer Space Treaty);

(3) establishing a military base or installation on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(4) testing of any weapons on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(5) conducting military maneuvers on the moon or other celestial bodies (Article IV, paragraph 2, Outer Space Treaty);

(6) carrying out nuclear weapons explosions in outer space (Article I.1(a), Limited Test Ban Treaty);

(7) military or hostile use of environmental modification techniques that could produce a widespread adverse effect in either the earth's atmosphere or outer space (Articles I and II, Environmental Modification Convention).

89. Carl Rochelle, *Coming Soon: Global Navigation for Consumers,* March 29, 1996, www.cgi.cnn.com/US/9603/global_satellite/index.html.

90. White House Fact Sheet, U.S. Global Positioning System Policy, March 29, 1996, http://gauss.gge.unb.ca/policy/Fact_Sheet.

91. *Id.*

92. The Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water ("The Test Ban Treaty"), *signed in Moscow* August 5, 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43, T.I.A.S. 5433 (*entered into force* October 10, 1963).

93. 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205, *signed in* Washington, London, and Moscow on January 27, 1967. Its full title is actually much longer: "The Treaty on Principles

Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." This treaty was a byproduct of the Legal Subcommittee of COPUOS and was largely based on the Declaration of Legal Principles governing the Activities of States in the Exploration and Use of Outer Space, which had been adopted in 1963 by General Assembly Resolution 1962.

94. *See* Andem, *supra* note 80, at 339; *see also* MENON, *supra* note 65, at 43; Peter Jankowitsch, *Legal Aspects of Military Space Activities*, SPACE LAW DEVELOPMENT AND SCOPE 143, 146 (1992).

95. UN General Assembly Resolution 1884 (XVII) was approved by acclamation on October 13, 1963. *See* MENON, *supra* note 65, at 40. It was one of the earliest efforts to provide international legal guidance which related to the issue of interference with space systems. The Declaration was a UN effort to restrict a future arms race in space, even though the resolution had no binding legal effect. It set forth the principles of co-operation and mutual assistance, calling for nations to conduct their activities in outer space with due regard for the interests of other nations, it then stated the following about interference with space systems:

> If a State has reason to believe that an outer space activity or experiment planned by it or its nationals would cause potentially harmful interference with activities of other States in the peaceful exploration and use of outer space, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State which has reason to believe that an outer space activity or experiment planned by another State would cause potentially harmful interference with activities in the peaceful exploration and use of outer space may request consultation concerning the activity or experiment.

While not prohibiting "harmful interference," the 1963 Declaration required prior consultations before a State could lawfully engage in that activity. The language of the Declaration, however, only protected activities from interference that were consistent with "the peaceful exploration and use of outer space." While clearly such general language could be seen as a limitation on some information operations, it would not preclude all information operations, especially those in response to an aggressive, hostile act of another State that was clearly outside the bounds of "peaceful exploration and use of outer space." Information operations in self-defense, for example, would not contravene the 1963 Declaration of Principles.

96. Gyula Gal, *The Peaceful Uses of Outer Space – After the Space Treaty*, PROCEEDINGS OF THE TENTH COLLOQUIUM ON THE LAW OF OUTER SPACE 129 (1967); *see also* BRUCE A. HURWITZ, THE LEGALITY OF SPACE MILITARIZATION 137 (1986); Mark G. Markoff, *The Judicial Meaning of the Term "Peaceful" in the 1967 Space Treaty*, PROCEEDINGS OF THE ELEVENTH COLLOQUIUM ON THE LAW OF OUTER SPACE 34 (1968).

97. HURWITZ, *supra* note 96, at 138.

98. Article 89, 1982 United Nations Convention on the Law of the Sea, U.N. Doc. A/CONF. 62/122 (1982), 21 I.L.M. 126–354 (1982).

99. This does not mean to imply that an assertion of sovereignty can only be done by means of an expressed statement. Certainly a nation can take actions which clearly express an intention to assert ownership over another nation's sovereign territory. However, the situation at issue here is a temporary interference with another nation's sovereign object. Actions that interfere with an object only *temporarily* are not likely to be construed as an assertion of sovereignty.

100. John C. Kunich, *Planetary Defense: The Legality of Global Survival*, 41 AIR FORCE LAW REVIEW 119, 129 (1997), *citing* W. Thomas Mallison, *The Laws of War and the Juridical Control of Weapons of Mass Destruction in General and Limited Wars*, 36 GEORGE WASHINGTON LAW REVIEW 308 (1967).

101. *See* Robert L. Bridge, *International Law and Military Activities in Outer Space*, 13 AKRON LAW REVIEW 649, 656 (1980) (referencing the Senate Foreign Relations Committee hearings on the Outer Space Treaty and the testimony of United Nations Ambassador Goldberg in response to

a question by Senator Carlson that a weapon of mass destruction "is a weapon of comparable ability of annihilation to a nuclear weapon, bacteriological . . . it does not relate to a conventional weapon.").

102. *See* Report of the Secretary-General, Developments in the field of information and telecommunications in the context of international security, U.N.G.A. 54/213 (Aug. 10, 1999). In response to an invitation to inform the Secretary-General of its views and assessments, the Russian Federation stated that "the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction." Russia is also seeking support for a UN resolution "calling for new international guidelines and the banning of particularly dangerous information weapons. In comments submitted to the UN Secretary General published last month, Russia warned that information operations 'might lead to an escalation of the arms race.'" Bradley Graham, *Military Grappling With Guidelines For Cyber Warfare*, WASHINGTON POST, Nov. 8, 1999, at A10.

103. There is no official US government policy as to whether an information operation is a weapon of mass destruction. Anders Eriksson, a senior analyst with the Defence Research Establishment, Stockholm, Sweden, argues that information operations are neither weapons of mass destruction, nor disruption, but rather of "precision disruption." *See* Eriksson, *supra* note 6, at 1.

104. *See* Parkerson *supra* note 54 at 81. Within academic circles, there have been two primary views on whether the peaceful purposes language should have application at all to activities in outer space since the express reference to peaceful purposes is limited to "the moon and other celestial bodies." Those who advocate the broader interpretation look to other pertinent clauses in the preamble of the Outer Space Treaty. Advocates of a narrow interpretation note that when the treaty drafters wanted a provision to apply to outer space in other articles, they specifically used the words "outer space." Thus, the *absence* of the term "outer space" in the second part of Article IV, dealing with "peaceful purposes," is even more telling. *See* Morgan, *supra* note 19, at 300.

105. During the drafting of the Outer Space Treaty, delegations from India, Iran, Austria, Japan, Brazil, and Mexico tried to include language that would completely demilitarize outer space, but their proposals were rejected by both the Soviet Union and the US. Kunich, *supra* note 100, at 137; Parkerson, *supra* note 54, at 82.

106. *See* Morgan, *supra* note 19, at 240–241. The US view has been that use of outer space for self-defense constitutes a "peaceful purpose." *Id.* at n. 366. In addition, use of communication, navigation, remote sensing, and reconnaissance satellites have also become an accepted practice considered to be for "peaceful purposes." *Id.* at 308, 317.

107. *See* Douglas S. Anderson, *A Military Look into Space: The Ultimate High Ground*, ARMY LAWYER 19, 28 (1995); *see also* Morgan, *supra* note 19, at 299.

108. An excellent example is that cited by Parkerson *supra* note 54, at n. 99, referring to Professor Bin Cheng, who in stating that the treaty's language provides that "Antarctica shall be used for peaceful purposes only," fails to mention the additional clarifying language not included in the Outer Space Treaty. Antarctic Treaty, *done at* Washington, December 1,1959, 12 U.S.T. 794, 402 U.N.T.S. 71, T.I.A.S. 4780 (*entered into force* on June 23, 1961). Similarly, the UN Convention on the Law of the Sea also provides that the high seas shall be reserved for "peaceful purposes," yet there has been no attempt to prohibit military ships from the high seas. The practice of nation States demonstrates that the non-aggressive use of the high seas is consistent with a peaceful purpose. *See* Parkerson, *supra* note 54, at 84.

109. Parkerson, *supra* note 54.

110. Statement by the President of the United States on International Cooperation in Space, *reprinted in* Senate Committee on Aeronautics and Space Sciences; *see also* Kunich, *supra* note 100, at 136–137.

111. 42 US Code sec. 2451(a).

112. *See* Kunich, *supra* note 100, at 131; Anderson, *supra* note 107, at 27; Parkerson, *supra* note 54, at 82; Bridge, *supra* note 101, at 658.

113. See Bridge, *supra* note 101, at 658.

114. A more extreme view is held by Professor Mark G. Markoff, Professor of International Law, University of Fribourg, Switzerland, who believes that the Outer Space Treaty was intended to completely demilitarize space. According to Professor Markoff, all parties to the Outer Space Treaty have agreed, through Article I, not to engage in any space activity that is not in the common interest of all other nations. Since any military activity, even that for self-defense or other non-aggressive purposes, cannot be for the benefit of all nations, the Outer Space Treaty does not authorize any military activity in outer space. *See* Anderson, *supra* note 107, at 26; Parkerson, *supra* note 54, at 83.

115. *See* Parkerson, *supra* note 54, at 82; Morgan, *supra* note 19, at 303.

116. Rymn James Parsons, *The Fight to Save the Planet: U.S. Armed Forces "Greenkeeping" and Enforcement of the Law Pertaining to Environmental Protection During Armed Conflict*, 10 GEORGIA INTERNATIONAL ENVIRONMENTAL LAW REVIEW 441, 470 (1998). Historically, treaty obligations between belligerents were suspended during armed conflict between them. 2 OPPENHEIM'S INTERNATIONAL LAW: A TREATISE 302 (H. Lauterpacht ed., 7th ed. 1952). Currently, the compatibility of particular treaties during a state of armed conflict is assessed on a case-by-case basis. D. P. O'CONNELL, 1 INTERNATIONAL LAW 268 (2d ed. 1970); RESTATEMENT (THIRD), FOREIGN RELATIONS LAW OF THE UNITED STATES, sec. 336, Reporter's Notes, 221–22 (1986).

117. Many might argue that copying, diverting, modifying, or otherwise tampering with data of another does constitute "harm" and would be a violation of international law.

118. S.C. Res. 678 (Nov. 29 1990).

119. S.C. Res 1264 (Sept. 15 1999).

120. GOLDMAN, *supra* note 59, at 28. The organization had its beginnings in 1865 when co-operative regulations were initiated by the Geneva Telegraphic Convention in Paris. That first agreement was modified and extended, culminating in the ITU in 1932 as a result of the combining of similar conventions. *See* 1 MANUAL ON SPACE LAW 225, n. 1 (Nandasiri Jasentuliyana and Roy S.K. Lee eds., 1979).

121. GOLDMAN, *supra* note 59, at 28.

122. 1 MANUAL ON SPACE LAW, *supra* note 120, at 196.

123. SPACE LAW DEVELOPMENT AND SCOPE 23 (Nandasiri Jasentuliyana ed., 1992).

124. The US signed the Convention on December 22, 1992, and signed the 1994 amendments at Kyoto on October 14, 1994. For a discussion of the 1992 ITC and 1994 amendments, *see* Marian Nash (Leich), *Contemporary Practice of the United States Relating to International Law*, 91 AMERICAN JOURNAL OF INTERNATIONAL LAW 93 (1997).

125. Annex, para. 1003 of the 1992 ITC. This language is identical to that found in Annex 2, para. 2003 of the 1982 ITC.

126. Eilene Galloway, *International Institutions to Ensure Peaceful Uses of Outer Space*, IX ANNALS OF AIR & SPACE LAW 323 (1984).

127. The US position, according to Michael W. Zehner, Air Force Deputy General Counsel (International Affairs), follows the more restrictive language of the ITC provision. Interview with Mr. Zehner (Dec. 20, 1999).

128. *Supra* note 116. An interesting comparison can be made to virtually identical non-interference language contained in the 1982 UN Convention on the Law of the Sea (LOS Convention). In Article 19(2)(k), the LOS Convention prohibits "any act aimed at interfering with any systems of communication" during innocent passage in a foreign territorial sea. No one has argued that similar non-interference provisions contained in the LOS Convention apply during periods of lawful military activity.

129. GOLDMAN, *supra* note 59, at 50; *see also* Morgan, *supra* note 19, at 253.

130. GOLDMAN, *supra* note 59, at 53.

131. *Id.* at 50.

132. *Id.* at 53.

133. *Agreement Reached on Intelsat,* SPACE DAILY, Feb. 13, 1998, at 2; *see also* Morgan, *supra* note 19, at 293–94.

134. The former Defense Communications Agency (DCA), now called the Defense Information Systems Agency (DISA), concluded that although there is no restriction on the military use of "specialized" services, all currently offered INTELSAT services are considered "public telecommunications services" available to military forces for military purposes. Morgan, *supra* note 19, at 293–94.

135. Letter of Warran Y. Zeger, Vice President, Law Department, COMSAT World Systems Division (Feb. 3, 1989) (on file with authors). COMSAT is a public and private satellite corporation created by Congress in 1962 by the Communications Satellite Act, 47 US Code 701 *et seq,* and is the US representative to both INTELSAT and INMARSAT. *See* GOLDMAN, *supra* note 59, at 50. It is regulated by the Federal Communications Commission (FCC) and receives its instructions on how to vote on INTELSAT and INMARSAT issues from the US government. *See* Morgan, *supra* note 19, at n. 291.

136. Agreement Relating to the International Telecommunications Satellite Organization, 23 U.S.T. 3813, T.I.A.S. No. 7532 (1973).

137. For example, Article III sets forth the organization's prime objective to be that "the space segment required for international public telecommunications services . . . be available on a non-discriminatory basis to all areas of the world." Thus, interference through information operations with multidirectional channels such as telex, telephony, and data transmission would affect the availability on a non-discriminatory basis of international public telecommunications. *See,* Martin A. Rothblatt, *Satellite Communication and Spectrum Allocation,* 76 AMERICAN JOURNAL OF INTERNATIONAL LAW 56, 64 (1982).

138. *Supra* note 116.

139. SPACE LAW DEVELOPMENT AND SCOPE, *supra* note 123, at 102; *see also* 1 MANUAL ON SPACE LAW, *supra* note 120, at 441.

140. Unlike INTELSAT, which is limited in its membership to ITU members, INMARSAT is open to all nations. SPACE LAW DEVELOPMENT AND SCOPE, *supra* note 123, at 102.

141. *Id.* at 102; *see also* GOLDMAN, *supra* note 59, at 58.

142. Convention on the International Maritime Satellite Organization, *opened for signature* Sep. 3, 1976, 15 I.L.M.1051 (1976) (entered into force July 1976).

143. Guidelines for INMARSAT Convention, Article 3(3) (March 29, 1988), (filed with INMARSAT following consultation with Argentina, Belgium, Brazil, France, India, Italy, Japan, Netherlands, Oman, Singapore, UK, and USA), *reprinted in* Memorandum of Law on The "Peaceful Purposes" Requirement and Inmarsat use by Armed Forces, Wolf D. Von Noorden, Special Counsel to INMARSAT, June 29, 1994, *cited in* Walter Gary Sharp, Sr., *Revoking an Aggressor's License to Kill Military Forces Serving the United Nations: Making Deterrence Personal,"* 22 MARYLAND JOURNAL OF INTERNATIONAL LAW AND TRADE 1, n. 221 (1998).

144. Neal T. Kilminster, COMSAT General Counsel opinion (April 15, 1999) (on file with authors).

145. *Id.*

146. *Id.*

147. *Id.* at 2.

148. Article XV(2), Strategic Arms Limitation Talks (SALT II), Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms, June 18, 1979; Article IX(2), Treaty Between the United States of America and

the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START), July 31, 1991.

149. Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL LAW REVIEW 57, 59 (1998).

150. Draft Joint Services Law of War Manual, para. 2.001 (unpublished 2d draft)[hereinafter LOW Manual]. Access to this draft is limited since it is still pending coordination and review.

151. Military necessity is codified in Article 23, para. (g) of the Annex to Hague IV, which forbids a belligerent "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war." For an excellent discussion of this principle, including a historical perspective, see LOW Manual, *supra* note 150, at Chapter II.

152. DoD/GC Paper, *supra* note 62.

153. International and Operations Law Division, Office of The Judge Advocate General, Department of the Air Force, LAW OF ARMED CONFLICT TRAINING GUIDE (April 1993).

154. DoD/GC Paper, *supra* note 62.

155. Law of war treaties contain the caveat that the right of a party to a conflict is not unlimited in its selection and use of means or methods of war. The principle of avoiding the employment of arms, projectiles, or material of a nature to cause *superfluous injury*, also referred to as *unnecessary suffering*, is codified in Article 23 of the Annex to Hague IV. LOW Manual, *supra* note 150, at para. 2.003.

156. INTERNATIONAL LAW – THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, (AFP 110-31) 1–6, *cited in* Ariane DeSaussure, *The Role of the Law of Armed Conflict During the Persian Gulf War: An Overview*, 37 AIR FORCE LAW REVIEW 46–47 (1994).

157. DoD/GC Paper, *supra* note 62.

158. The Judge Advocate General's School, Operational Law Handbook 5-5 (2000).

159. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I), art. 48, 1125 U.N.T.S.

160. *See* DoD/GC Paper, *supra* note 62. *See generally*, Protocol I, *supra* note 159, art. 43.

161. DoD/GC Paper, *supra* note 62. *See generally*, Geneva Convention Relative to the Treatment of Prisoners of War, art. 4(2)(b).

162. DoD/GC Paper, *supra* note 62.

163. AFP 110-31, *supra* note 156, para. 6-3a.

164. DoD/GC Paper, *supra* at note 62.

165. *Id.* at 6, 8.

166. Primer on Legal Issues in Information Operations, *supra* note 27, at 19.

167. DeSaussure, *supra* note 156, at 46–47.

168. LOW Manual, *supra* note 150, at para. 2.005.

169. DeSaussure, *supra* note 156, at 47.

170. DoD/GC Paper, *supra* note 62. Of course, ruses and the use of the element of surprise are not illegal acts. *See* LOW Manual, *supra* note 150, at para. 2.006.

171. Department of Defense, Doctrine for Joint Operations, JOINT PUB 3-0, (Feb. 1, 1995).

172. *See* Scott, *supra* note 149, at 60.

173. DoD/GC Paper, *supra* note 62. *But see* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 AIR FORCE LAW REVIEW 217 (1999); SHARP, *supra* note 6, at 125–133.

174. This is largely a recognition of the international law doctrine called *"tu quoque,"* in which "a nation has no standing to complain about a practice in which it itself engages." DoD/GC Paper, *supra* note 62.

175. This assumes that Nation A and Nation B are parties to those formerly bilateral agreements.

176. None of these agreements has any specific provision that indicates whether the parties intended that they apply during international armed conflict. It also appears that their provisions on harmful interference are inconsistent with a state of hostilities. *See* DoD/GC Paper, *supra* note 62.

177. RICHARD J. ERICKSON, LEGITIMATE USE OF MILITARY FORCE AGAINST STATE-SPONSORED INTERNATIONAL TERRORISM 144–145 (1989).

178. *Id.* at 144–146. The *Caroline* case is frequently cited as precedent in the customary international law of self-defense. A ship named the *Caroline* would periodically sail from the US to Canada to resupply the rebels there during Canada's 1837 revolt against the British. The British responded by entering the US, seizing the offending ship, and destroying it. The British claimed they acted in self-defense. Through correspondence with the British government on the incident, Secretary of State Daniel Webster set forth his understanding of the conditions necessary for self-defense. According to Webster, there "must be a necessity of self-defense, instant, overwhelming, leaving no choice of means and no moment for deliberation." Moreover, the act should involve "nothing unreasonable or excessive, since the act justified by the necessity of self-defense must be limited by that necessity and kept clearly within it." Webster's criteria of "necessity" and "proportionality" continue to form the basis of a lawful claim of self-defense. OPPENHEIM'S INTERNATIONAL LAW 420 (Robert Jennings and Arthur Watts eds., 9th ed. 1933); *see also* Richard G. Maxon, *Nature's Eldest Law: A Survey of a Nation's Right to Act in Self-Defense,* PARAMETERS, Autumn 1995, at 55, 56–57.