Legal Aspects of Offensive Information Operations in Space

THOMAS C. WINGFIELD*

The electron is the ultimate precision guided munition.
-John Deutch, Director,
Central Intelligence Agency

They couldn't hit an elephant at this dist—
-General J. Sedwick
(Last words at the Battle of Spotsylvania, 1864)

Introduction

The law of information conflict is the extension of traditional national security law in the new realm of cyberspace. This extension has greatly expanded the scope and complexity of national security law, adding portions of numerous other disciplines: intellectual property, telecommunications, and domestic criminal law, among others. These additions reflect the new weapons, targets, and soldiers operating on this new battlefield.

The principal intellectual challenge in the law of information conflict is deciding which areas can be covered by the mere extension of conventional legal principles to cyberspace by analogy, and which require whole new methodologies. One of the most contentious areas, both analytically and militarily, will be offensive information operations in space.

Department of Defense Directive S-3600.1 defines information operations as "actions taken to affect adversary information and information systems while defending one's own information, and information systems."[1] Wald and Federici describe the qualities of an information system which may be compromised by such actions:

> *confidentiality*—the assurance that information will be available only to authorized participants…*availability*—the assurance that information system services will be available when needed [and]…*integrity*—the assurance that unauthorized parties cannot change the information in a system or forge the identity of the originator.[2]

The purpose for threatening these attributes of an enemy's information systems is stated in *Joint Chiefs of Staff Joint Publication* 3-13, *Joint Doctrine for Information Operations* (*Joint Publication* 3-13):

> the ultimate strategic objective of offensive IO is to affect adversary or potential adversary decision makers to the degree that an adversary will cease actions that threaten US national security interests. At the tactical, operational and strategic levels, IO target and protect information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems.[3]

This same thought was expressed during the Second World War by Captain Sir Basil Liddel Hart: "[t]he real target in war is the mind of the enemy commander, not the bodies of his troops."[4]

The purely military application of Information Operations is Command and Control Warfare, also called "C2W." It is defined by *Joint Publication* 3-13 as:

> [t]he integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations.[5]

Information operations can have a devastating effect on the United States or a potential adversary. As critical infrastructures around the world (power distribution, telecommunications, banking, emergency services, transportation, and national defense, among others) take advantage of the efficiencies offered by rapid advances in information technology, these same infrastructures become more dependent on these systems and more vulnerable to information attack. Now, everything from national stock exchanges to national air traffic control systems are at risk.

The two key components of these advances are the high speed of information processing and the global networking of these systems. This second factor is made possible by the ground based international telecommunications infrastructure and a growing constellation of satellites which provide countries with a means to acquire and transmit information for military and civilian purposes. These satellites are vital, vulnerable nodes—making them high-value targets in any future information conflict.

This paper will examine the range of possible offensive information operations in space: intelligence collection, operations *through* satellites, and operations *against* satellites. The second section will describe the types of offensive space operations. The legal regime, running from the peacetime framework of the United Nations (UN) Charter and space treaties to the law of war, will be described in the third section. Finally, the paper will review an analysis applicable to all types of offensive information operations in space. The goal of this paper is to provide a broad, comprehensive framework within which to evaluate fact-driven legal questions on specific offensive information operations in space. Due to the highly classified and compartmented nature of such operations, I have chosen to examine the entire *theoretical* range of such operations, without speculation on the real-world capabilities or intentions of any nation.

Operations

The first step in analyzing the legality of offensive information operations in space is to develop a taxonomy for describing them.[6] For ease of analysis, this field may be divided into three broad areas: intelligence collection, offensive information operations *through* satellites, and offensive information operations *against* satellites.

Intelligence Collection

Collection Against Platforms. The two principal types of intelligence collection involving space platforms are those collection operations *against* a given platform, and those *through* a given platform. Platform reconnaissance against a satellite may be accomplished at four levels of intrusiveness: passive collection, active or intrusive collection, installing trapdoors, and planting Trojan Horses.

Passive collection operations involve observing a satellite (usually photographically) or monitoring its radio or other electronic emissions. This type of collection, requiring the least technical sophistication, is analogous to a police officer staking out a suspect's home from across a street, observing only those details the suspect reveals to the public.

Active or intrusive collection became possible with recent advances in computer technology, enabling an adversary to "hack" into an opponent's satellite in order to collect intelligence from the inside. In a police analogy, this would be the equivalent of the police entering the suspect's home while he is away.

Installing trapdoors is the next level of intrusiveness. Here, the adversary leaves a hidden code in the space platform's software that only he can activate, enabling him to gain fast, simple, and stealthy access to the enemy

system in the future. These operations are similar to the police obtaining a copy of the suspect's house key, permitting rapid reentry at any time.

Planting Trojan Horses is the most intrusive sort of intelligence collection. This method involves leaving behind a code that does not merely grant repeat access, but that will at some time in the future do actual harm to the system. This code, dormant and hidden in peacetime, may be activated in wartime if certain programmed criteria are met or, if the adversary has a trapdoor, by an affirmative command. These operations are similar to the officers staking out a violent suspect's home from the inside, ready to surprise him when he returns home and use force to subdue him. To be effective, the actual *planting* of such a Trojan Horse must be done without the adversary's knowledge and without affecting his information operations. It is only in time of crisis or during armed conflict, when the wartime criteria are met or the command is given, that this potential capability becomes an information operation under the Department of Defense definition. This is the point at which intelligence collection transitions to offensive operations.

Collection Through Platforms. The four previously described types of intelligence collection are all aimed at the platform *per se*. The other broad category of collection is "piggybacking," which is altogether different. Here, the intelligence collection target is not the satellite, but the satellite's own target. By piggybacking, the adversary receives the same information as the satellite's unwitting owner--the same video images, the same signals intercepts. In this way, the adversary not only has increased his knowledge base, but knows precisely what intelligence information the satellite's owner is receiving. Undetected piggybacking, would require careful placement of intercept equipment in the downlink footprint, and sophisticated cryptographic algorithms, operating in near-real-time. Completing the police analogy, the police have planted a wiretap in the office of a crime boss meeting with his informants and are able to listen in on what that boss knows about the police investigation.

Offensive Operations *Through* Satellites

Offensive information operations that simply use a satellite as a means to reach another, terrestrial target—also known as taking a "bank shot,"—require two levels of analysis. The primary analysis is an application of the law of war to the attack on the terrestrial target. The secondary analysis is a review of space treaties to determine the legality of using a satellite in the operation. The more attenuated the role of the satellite in question, the greater the chance that international law will not be violated. To give two examples, a cyber weapon (perhaps a digital sequence intended to disrupt the operations of a target computer) routed, *intact*, through a satellite whose governing treaty forbids such use may be problematic. However, a cyber weapon which is merely *activated* by a simple, satellite-routed phone call, having reached its target through terrestrial communications links, may cause less difficulty. In any case, these two lines of analysis, for the target and for any satellite platform used in reaching it, are distinct.

Offensive Operations *Against* Satellites

A different analysis is required when the target *is* the satellite. There are five distinct types of offensive operations against satellites, and all involve analyses of their legality as targets under the law of war and under the special treaty regime of space law. The five are blinding, shutdown, movement, destruction, and appropriation or impressment.

Blinding. Blinding operations include anything from a temporary "dazzling" with a laser to a permanent burnout of optical or other receivers with an intense energy burst. This type of attack would be directed toward intelligence collection satellites, and is intended to prevent them from gathering or relaying information to an enemy.

Shutdown. In shutdown operations, the adversary gains access to a satellite's control program and directs that it cease functioning for some length of time. Again, this may be for only the first few critical moments of a terrestrial attack, or a permanent command to never resume operations. While not physically damaging the

satellite, it does deprive its owner of its use during precisely the period when it is most needed. Clearly, a permanent shutdown command is tantamount to loss of the platform, especially for any owner not able to reaccess the platform and remove the overriding code.

Movement. In space, all movement is described in two elements, attitude and translation. Attitude refers to the direction a satellite points; translation is its actual movement from one position to another. An attitude movement attack, then, may be mounted by accessing its control program and ordering a satellite to rotate on its axis, pointing it in another direction.[7] Such an attack would be effective against a photographic intelligence satellite whose effectiveness depends on pointing at precisely the right place for imaging a target.

More threatening is a translation movement attack, which involves activating a satellite's thrusters and sending it into a new orbit. In many respects, a satellite's orbit determines its usefulness—geostationary for whole-earth communications, very low for pinpoint intelligence collection, and, of course, a precise ground track to bring it over a high-priority collection target. Moving a satellite's orbit may put it on a collision course with another object in an intersecting orbit. Finally, the altitude of a satellite determines its longevity: at several hundred miles, it may stay aloft for centuries; under a hundred miles, it may last only days or even hours before reentering the atmosphere. For a small satellite, this would involve its complete destruction. For a large one, it would raise the additional legal issue of discrimination (discussed below), as the residue would slam into a largely undeterminable earth target.

Such a movement, in either attitude or translation, can also be permanent or temporary. A satellite may be momentarily turned away from a terrestrial attack in progress, or permanently lofted into a distant, useless orbit.

Destruction. Destruction may be an extension of movement, such as a command to translate to such a low orbit that the satellite burns up or crashes into the earth. It could be accomplished by the movement of the target or another satellite so that they collide in orbit. The platform could be attacked with anything from a high-tech laser to a closer but lower-tech cannon. The destruction could even be accomplished by an appropriate command to the satellite's control program, mismanaging its fuel temperature controls to the point of detonation. Destruction is the closest fit with traditional terrestrial military uses of force, and is perhaps the simplest in a purely analytical light.

Appropriation/Impressment. Although less physically damaging than destruction, appropriation or impressment is perhaps more harmful to an enemy. This technique is the offensive operations parallel to piggybacking, but involves a transfer of control to the adversary. The satellite's control program is accessed and altered, denying the launching state use of its own platform. Worse than mere destruction, however, the satellite's capabilities are then at the disposal of the attacking state. This is roughly comparable to a ship being captured at sea. Again, this technique could be temporary or permanent.

Legal Regime

The Law of Peace

The peacetime legal framework for offensive information operations in space is primarily a product of the UN Charter and four space treaties.

UN Charter. The UN Charter establishes principal thresholds for the use of force. The first is Article 2(4):

> [a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[8]

Article 2(4) sets a very low threshold for the use of force, creating a broad prohibition. The second, Article 51, deals with self-defense:

> [n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations….[9]

It is important to note that Article 2(4) prohibits the use of force, except that which is recognized as inherent under Article 51.

Article 51 sets a higher threshold permitting the use of force in self-defense and creating a narrow exception to Article 2(4). When the Article 51 threshold is met, a proportionate military response by the victim state would be a lawful exercise of self-defense. It is reasonable to assume that the threshold is also met when a threat of force becomes so credible, specific, and imminent that the aggressor's forces have been irrevocably committed to action, or when there remains insufficient time for indications and warning to exercise reasonable self-defense if an attack is launched.[10] The difference, then, between the Article 2(4) and 51 thresholds is that mere threats of force which do not support a lawful exercise of anticipatory self-defense are below the Article 51 threshold, but above the Article 2(4) threshold. To posit a use of force to which the victim state is not permitted to make a necessary and proportional response, however large or small that may be, is counterintuitive in the extreme.

The third, Article 39, describes the UN Security Council's central role in making these determinations:

> [t]he Security Council shall determine the existence of any *threat to the peace, breach of the peace, or act of aggression* and shall make recommendations, or decide what measures shall be taken…to maintain or restore international peace and security. [emphasis added][11]

The Security Council may find these conditions to exist at any point along the spectrum of conflict, even below the Article 2(4) threshold.[12]

Article 41 is the only article in the Charter which addresses, however tangentially, information operations:

> [t]he Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications, and the severance of diplomatic relations.[13]

Article 41 complements Article 39 in that it describes the Security Council's power to coerce member states to break contact with an offending state, isolating it as a sanction beneath the use of force. From the context of Article 41, it seems clear that "interruption" does not mean information operations carried out *within* the offending state, but merely the severance of its communications and other links with the outside world. Furthermore, this severance is to be accomplished not by acting against the offending state, but by authoritatively directing compliant member states to withdraw their connections from their side of the border.

Article 42 is the last step in this process. It provides:

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

The use of the phrase "such actions" allows the broadest possible latitude for military operations, avoiding the limitations of "use of force" or "armed attack." It seems that information operations at any level of intensity, provided they are carried out by a member state's military forces pursuant to Security Council request or instruction, would fit squarely within an Article 42 action.

While the Security Council could make an Article 39 determination that an act below the Article 2(4) threshold constitutes a threat to the peace, a breach of the peace, or an act of aggression, this is not likely in any plausible scenario. Information operations subtle enough in their effects to remain below the Article 2(4)

threshold would be difficult to detect and even more difficult to follow to their source. Until information operations begin to cause damage comparable to that caused by kinetic attacks, they may well escape decisive action by the Security Council.

Outer Space Treaty.[14] Against this background, four space treaties define the positive law environment for evaluating the legality of offensive information operations in space. The first of these is the Outer Space Treaty. In its preamble, it describes "the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes."[15] It further declares that space is "the province of all mankind," and, therefore, not subject to sovereign claims by any nation.[16] From this has evolved the concept of "peaceful purposes," aspirational here and mandatory in other treaties. Nowhere in the Outer Space Treaty is the term defined, and two opposing views have developed. The majority opinion, certainly among spacefaring nations, is that "peaceful" means "nonaggressive," a relatively high standard allowing for considerable military operations in space. The minority view, more common among the less advanced, non-spacefaring nations, is that "peaceful" means "nonmilitary," setting such a low threshold that even routine, peacetime military business, such as communications and weather observation, would be prohibited.

Article III of the treaty extends the application of international law, including the UN Charter articles on use of force, to outer space.[17] Article IV details specific prohibitions: weapons of mass destruction anywhere in space, and military bases, weapons testing, and maneuvers on the surface of any celestial body.[18]

State responsibility is governed by Articles VI and VII. Article VI makes states responsible for the actions of all of their nationals in space, and not merely government representatives.[19] Article VII assigns liability for damage caused by activities in space to the launching state.[20]

Article XI carries a notice requirement, instructing states to notify the office of the UN Secretary General of each space activity "to the greatest extent feasible and practicable."[21] This language creates a broad gray area within which notice of most if not all military activities in space are not reported in any detail. Finally, Article XII grants state parties the right of inspection of any facility located on the surface of another celestial body, but no access to orbital platforms.[22]

Liability Convention.[23] The second major space treaty is the Liability Convention, which sets a liability standard for activities in outer space, provides an exception to that standard, and details the procedures for pursuing a claim. The liability standard is bifurcated. On the surface of the earth or in its atmosphere, the launching state has absolute liability for damage caused by its platforms.[24] In space, the standard is simple negligence.[25] This standard is limited in one circumstance: if the damaged state acts with gross negligence or wilful intent, and the launching state acts in accordance with international law, there is no absolute liability for the launching state.[26]

To pursue a claim under the treaty, Articles VIII and IX require that the claim be submitted by a state through diplomatic channels.[27] Article IX adds the requirement that the claim be submitted within one year of the event or the discovery of the responsible state's identity.[28] Finally, Article X states that local remedies need not be exhausted before a claim may be made under the treaty.[29]

Under the law of war, a belligerent has no duty to pay for damage done to lawful targets. Where the Liability Convention has the greatest effect, though, is in peacetime information operations. A nation launching an offensive information operation in space would be liable to the launching state for the damage done to the satellite, and by the satellite as a result of the operation against it. For example, an operation which simply destroyed a space platform would leave the nation which conducted the operation liable for the value of the satellite. An operation which deorbited a satellite, sending it crashing into a terrestrial building, would be liable for that damage as well.

INTELSAT Agreement.[30] The third major treaty is the INTELSAT Agreement. It governs the use of INTELSAT communications satellites, which link fixed ground stations. The Agreement divides satellite services into two categories: "public telecommunications services" and "specialized telecommunications services."[31] Public telecommunications services include:

> [f]ixed or mobile telecommunications services which can be provided by satellite and which are available for use by the public, such as telephony, telegraphy, telex, facsimile data transmission, transmission of radio and television programs between approved earth stations having access to the INTELSAT space segment for further transmission to the public, and leased circuits for any of these purposes; but excluding those mobile services…which are provided through mobile stations operating directly to a satellite which is designed, in whole or in part, to provide services relating to the safety or flight control of aircraft or to aviation or maritime radio navigation….[32]

Specialized telecommunications services, on the other hand, include:

> telecommunications services which can be provided by satellite, other than those defined in paragraph (k) of this Article [*supra*], including, but not limited to, radio navigation services, broadcasting satellite services for reception by the general public, space research activities, meteorological services, and earth resource services.…[33]

Article III, on the scope of INTELSAT activities, contains two restrictions on "military purposes," not defined in Article I. Paragraph (d) allows the INTELSAT space segment "to be utilized for the purpose of specialized telecommunications services, either international or domestic, [for] other than military purposes.…"[34] Paragraph (e) states that "INTELSAT may. . .provide satellites or associated facilities separate from the INTELSAT space segment for. . .specialized telecommunications services, other than for military purpose . . . ."[35]

Taken together, it appears that the INTELSAT organization may offer "public telecommunications services" to the military of a nation, but not "specialized telecommunications services." Offensive information operations, routed through INTELSAT's public telecommunications services appear to be nonviolative of the Agreement.

INMARSAT Convention.[36] The fourth and final major treaty is the INMARSAT Convention. This treaty covers the use of INMARSAT communications satellites, which service mobile "ground" stations, such as ships at sea. Article 3(3) of the Convention states that "[t]he Organization shall act exclusively for peaceful purposes," but does not specifically prohibit military use in accordance with international law and the UN Charter. Again, a nonaggressive operation, legal under the Charter, would not violate the Convention.

Other Treaties. Beyond these four major treaties, several other international agreements tangentially affect offensive information operations in space. The International Telecommunications Convention of 1982, better known as the Nairobi Convention, contains several provisions relating to interference with transmissions. Article 19, paragraph 109, allows signatories to "stop the transmission of any private telegram" threatening to state security,[38] while paragraph 110 of the same article allows Member States to do the same to any private telecommunication appearing to pose such a threat.[39]

Article 20, paragraph 134, permits Members "to suspend all international telecommunication service" to their own country, provided they notify the UN Secretary General of the action.[40] Article 35, paragraph 158, requires that all "stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members…."[41] Article 38, paragraph 164, extends this provision to military radio installations, with a qualification: they must observe measures to prevent harmful interference, "so far as possible."[42] Annex 2 to the Convention defines harmful interference as that "which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio communication service…."[43]

The principal question under the Nairobi Convention is determining which portions remain in effect at which levels of hostility. Articles 19 and 20 deal only with a country's control over its *own* communications, and so are always in effect. Articles 35 and 38, with their prohibition of "harmful interference," are more problematic in international conflict. Clearly, essential humanitarian communications should continue to operate in wartime. Equally clearly, military and intelligence traffic would become legitimately vulnerable to attack. What is less clear is the gray area in between, in which some civilian communications would be interrupted in the process of affecting military transmissions. In a traditional military attack, it is relatively simple to drop bombs on a known military communications site and not drop bombs on a separate civilian radio station. With the advent of subtle information technology, however, it is now possible to discriminate in the same way by insinuating signals into mixed military-civilian facilities, targeting only those circuits or programs that are lawful targets. This technology, like the technology of precision guided munitions, may raise expectations and later legal standards for discrimination and reduction of collateral damage.

Beyond the Nairobi Convention, several other types of treaties affect the legal environment of information operations. Arms control treaties, such as the ABM Treaty, frequently contain prohibitions on "interference and concealment," in evading national technical means (NTM) of verification. NTM include national-level strategic reconnaissance platforms, primarily specialized aircraft and satellites. These prohibitions are designed to provide a confidence-building transparency and deter cheating. An offensive information operation, at least in peacetime, against a platform performing this sort of verification work would run afoul of these treaties. In wartime, these reconnaissance platforms would become lawful targets.

The Convention on International Civil Aviation, better known as the Chicago Convention, contains an additional limitation. Professor Gary Sharp explains:

> [a]s a result of the KAL 007 shootdown by the Soviets in 1983, the delegates to the International Civil Aviation Organization adopted article 3*bis*, which provides that "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of the persons on board and the safety of the aircraft must not be endangered." While article 3*bis* is not in force for the United States, the Legal

> Counsel for the Department of Justice opined in a formal memorandum of law dated 14 July 1994 that article 3*bis* is declaratory of customary international law.[45]

While it is difficult to imagine a scenario in which a civil airliner would be targeted in an offensive information operation, the possibility exists that damage to such an airliner could be sustained as a result of an attack on another target. The destruction of an adversary's Global Positioning System (GPS) satellite may result in degraded navigational information to military and civil aircraft alike. A more subtle attack may degrade the accuracy of the navigational information below the level useful for military targeting, but maintain a level necessary for civilian airliners' safety of flight. To the extent that such an effect is foreseeable, it must be taken into account in planning such an operation.

Many stationing arrangements, such as the Status of Forces Agreements (SOFAs) the United States has with numerous allies, have provisions on the coordination required to launch offensive (distinct from "aggressive") operations from the host country's soil. A legal factor to be considered is whether or not the contemplated operation is governed by such an agreement. Perhaps more important, the political ramifications of launching such an operation could be immense, particularly if the government of the host nation were unwitting of the capability resident within its borders.

The last such agreements are the contracts governing the use of the new cellular constellations. These voice and data networks, such as Iridium and Teledesic, each consisting of dozens of satellites, permit instantaneous communications from any cellular phone user to any other cellular phone user, anywhere on the planet. Obviously concerned with the effect of military interference into such a network and the prospect of their satellites becoming lawful targets in time of war, the owners of these constellations may place contractual obligations on governments using their systems—obligations that may limit offensive information operations through them.

Domestic Law. Domestic law intrudes on offensive (usually extraterritorial) information operations far less than it does on defensive operations. However, there are some limitations. 47 U.S.C. § 502 provides domestic criminal penalties for violating international telecommunications restrictions,[46] while 18 U.S.C. § 1367 does the same for "whoever, without authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission."[47] There are two principal questions about the applicability of section 1367. First, did Congress intend for the statute to reach extraterritorially, protecting foreign-owned satellites? Second, does the exception for any "investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the US" allow for military interference with such transmissions? If the answer to the first question is no, then the second question is moot. However, if the statute is intended to reach beyond the U.S., then the breadth of the exception is key.

Information operations, by their very nature, may often be conducted as covert actions. According to the U.S. Atlantic Command Memorandum 5800 J02L, dated 16 January 1996:

> [e]ven during armed conflict, covert actions, which are defined as activities "where it is intended that the role of the United States government will not be apparent or acknowledged publicly," must be approved through a Presidential finding, under 50 USC 413b. Excluded from the definition of "covert action," however, are "traditional…military activities…." (50 USC 413(e)).[48]

The precise line between traditional military activities and standard covert actions, particularly in this new area, is not yet clear. Given the ultra-sensitive nature of such operations, it is likely that any offensive information operation in space will be coordinated through the National Command Authorities (NCA) whether it is to be carried out by a civilian or a military agency.

Domestic Policy. Domestic policy on offensive information operations in space is narrow and focused. There are four primary documents on point. The first is *Department of Defense Directive* S-3600.1, *Information Operations (IO)*, dated 9 December 1996. This foundational directive provides definitions of terms, codifies institutional relationships, and places information operations within the context of other military operations.[49] The

second, *Chairman of Joint Chiefs of Staff Instruction*, CJCSI S-3210, *Joint Information Warfare Policy*, dated 2 January 1996, outlines the coordination process for approval of information operations. For offensive information operations, that approval must almost always come from the National Command Authorities, comprised of the President and the Secretary of Defense.[50] *Department of Defense Instruction* 5000.1, *Defense Acquisition*, dated 15 March 1996, requires that all new weapons undergo a legal review for compliance with domestic and international law.[51] In addition, *Department of Defense Directive* 5100.77 requires that new tactics, techniques, capabilities, or rules of engagement (ROE) for existing weapons receive a legal review.[52] This is actually more problematic than it would appear, because many information "weapons" are simply electronic streams of "1s" and "0s." These weapons have evolved as new capabilities of existing platforms or equipment, and so may not have undergone a *de novo* legal review. An additional problem is that the existence and capabilities of such weapons would undoubtedly be so highly classified, and so tightly compartmented, that the number of cleared and briefed attorneys to conduct such reviews would be greatly limited.

The Law of War

The first task in applying the law of war to a military operation is determining when to apply it. Much offensive information operation may be carried out in peacetime, and the most intrusive of these, Special Information Operations, are treated as traditional covert actions and coordinated as such with the NCA. Still, at some point, the conduct of offensive information operations in space may theoretically go beyond the plausibly deniable single act and become the functional equivalent of a use of force.

To make this determination, one must start with the standards of the UN Charter. Article 2(4) sets a very low standard, but does not precisely define what is meant by a "threat or use of force against the territorial integrity or political independence of any state."[53]

Common Article 2 of the four Geneva Conventions of 1949 is slightly more specific. It calls for the Convention (and by customary extension, the law of war) to apply in any of three cases:

> the present Convention shall apply to all cases of declared war or any other armed conflict….The Convention shall also apply to all cases of total or partial occupation of the territory of a High Contracting Party….[54]

Of the three cases, declared war and total or partial occupation are relatively easy to spot. The second case, "any other armed conflict," is far more difficult. Jean Pictet, author of the *Commentary on the Geneva Conventions*, devised a "scope, duration, and intensity" test to serve as a guide. Desiring to have the protections afforded by the Conventions, and the customary law of war in general, apply at the lowest possible level of conflict, Pictet made this test disjunctive. If any single military operation, or group of operations, were carried out beyond a certain geographical scope, or beyond a certain temporal duration, or beyond a certain intensity of violence, then the nation conducting that operation would be a party to an armed conflict.[55] This would bring the operation under the aegis of the Conventions and the law of war.

The level of violence in any offensive information operation in space may be evaluated by passing it through the analytical lens of Pictet's "scope, duration, and intensity" formulation. While this analysis is evolving from the disjunctive (a high value for any of the three components resulting in a state of belligerence) to the conjunctive (belligerence requiring a high value in *each* of the three components), the underlying elements remain the leading measure of the violence of actions.

Pictet's Commentary. Scope describes the breadth of the attack, and is best divided into an analysis of the weapon and the target. For the weapon, the two key components are the number used (e.g., a single, stealthy unit or a massed invasion) and the nature of the weapon itself (e.g., a mere radio message activating an altered control program or a Death Star-like blast from a powerful laser cannon).

As for the target, the same two factors come into play: the number of platforms attacked (e.g., a single satellite gone offline or an entire constellation stopped reporting), and their nature (e.g., a redundant weather satellite gone down or the key platform in a ballistic missile launch reporting network disappeared). The number and nature of weapons used and targets attacked define the scope of the attack.

Probably the simplest of the three criteria to evaluate, duration consists of the quantity *and* the quality of the time the launching state is denied the use of its satellite. Quantitatively, any attack's effects are either temporary or permanent, and temporary attacks can be further described by the number of minutes, hours, or days they persist. Qualitatively, it is the criticality of the time the platform is unavailable to the launching state that matters. Thirty days without a backup cellular retransmission satellite may be less threatening than thirty minutes without an ICBM early warning platform.

Intensity, in this context, can be described by a spectrum. At one end are operations that have no effect on the launching state's use of its satellite, and at the other are operations that completely deny such use. This "mission permissive/mission coercive" dichotomy becomes complex in the center of the spectrum, as an adversary seeks to manipulate the flow of data through a satellite still being used by its owners. Indeed, destruction of the platform may cause less damage, in the long run, to a launching nation than continuously receiving a steady stream of subtly altered data. So, while the degree to which the original mission continues is a helpful measure of intensity, it must be balanced with an examination of the actual damage done downstream.

Pictet's criteria of scope, duration, and intensity are extremely useful in determining the general applicability of the law of armed conflict. It must be remembered, however, that there are situations below the level of continuing belligerency which demand a proportionate, discriminate, and chivalrous use of force in self-defense. The absence of generalized hostilities may prevent the complete application of the law of armed conflict, but it would not relieve the defending state from responding in accordance with the principles below.

Proportionality. The principle of proportionality demands that "the loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained."[56] Proportionality is the balancing of military necessity and unnecessary suffering.[57]

Under the principle of military necessity, "only that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources may be applied."[58] Unnecessary suffering results from "the employment of any kind or degree of force not required for the purpose of the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources," and is prohibited.[59] At the two extremes, military necessity does not permit any activity which is specifically forbidden by international law, and purely unnecessary suffering may never be imposed. In the large gray area in-between, they are to be balanced in light of the best information available to the commander at the time the operation is planned and executed.

In the area of offensive information operations, downstream effects may produce unintended consequences. During the Persian Gulf War, the Coalition targeted and destroyed large portions of the Iraqi power grid. Military necessity appeared to outweigh the inconveniences to the Iraqi civilian population. Unbeknownst to Coalition targeteers, Baghdad's sewerage system required electric pumps to operate (unlike gravity-driven systems in most of the civilized world). When the power grid came down, the sewer pumps ceased to function, and the standing waste posed a serious health threat to Iraqi civilians.[60] While the understandable lack of sewerage intelligence may have left this result reasonably unforeseeable, it is suggestive of the potential ripple effects of information attacks in the future. The technology available to those planning such operations will determine the precision with which such effects may be calculated.

Discrimination. The principle of discrimination restricts methods, weapons, and targets. In addition to technical proscriptions against attacking certain types of property, the principle requires that belligerents distinguish "between combatants, who may be attacked, and noncombatants, e.g. civilians, who may not be attacked."[61] The Regulations Annexed to Hague Convention IV (Hague Regulations) limit the permissible civilian effects of information attacks. One particular limitation has an application to offensive information operations in space. Article 53 states:

> [a]ll appliances, whether on land, at sea, or in the air, adapted for the transmission of news, or for the transport of persons or things...may be seized, even if they belong to private individuals...but must be restored and compensation fixed when peace is made.[62]

It appears that in time of war, at least some satellites may be considered such an appliance for the purposes of this Convention. Unlike other lawful targets, however, these satellites' loss would have to be compensated once hostilities had ceased.

Chivalry. "Dishonorable (treacherous) means, dishonorable expedients, and dishonorable conduct during armed conflict are forbidden."[63] Chivalry, in the context of the law of war, deals with the line between *ruses of war*, which are deception of the enemy by legitimate means,[64] and *perfidy* (treachery), which is not.

Article 24 of the Hague Regulations states: "[r]uses of war and employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[65] Article 37(2) of Protocol Additional to the Geneva Conventions (Protocol I) states:

> [r]uses of war are not prohibited. Such ruses are acts intended to mislead an adversary to induce him to act recklessly but which infringe no rule of [the law of war] and which are not perfidious because *they do not invite the confidence of an adversary with respect to protection under that law*. The following are examples of ruses: the use of camouflage, decoys, mock operations and misinformation.[66] [emphasis added]

Air Force Pamphlet 110-31, *International Law—The Conduct of Armed Conflict and Air Operations*, list numerous lawful ruses which can be easily analogized to information operations:

> surprises, ambushes, feigning attacks, retreats, or flights; simulation of quiet and inactivity; use of small forces to simulate large units; transmission of false or misleading radio or telephone messages (not involving protection

> under international law such as internationally recognized signals of distress); deception by bogus orders purported to have been issued by the enemy commander; use of the enemy's signals and passwords; feigned communication with troops or reinforcements which have no existence, and resort to deceptive supply movements.[67]

Perfidy, on the other hand, is a war crime. Article 37(1) of Protocol I defines perfidy as:

> [a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the [law of war], with intent to betray that confidence….[68] The classic example of perfidy is the use of a white flag of surrender to draw an enemy out of cover, as the Argentineans did during the Falklands War, to then open fire on them. Using a protected symbol, such as the Red Cross, as cover for military operations, would be another example.

Information operations, by their very nature, are designed to manage an adversary's perceptions, subtly altering his or her view of reality. Because of this, these operations frequently straddle this line. They are permissible up to the point that they falsely promise a specific legal protection to a manipulated adversary. By way of example, if an image of Slobodan Milosevic were digitally morphed to show him addressing his troops on television, telling them to lay down their arms because a truce has been called, and then NATO troops opened fire on these same troops, the NATO action would be perfidious—if it falsely promised the specific legal protections accorded to combatants during a truce. If, however, Milosevic's television image were digitally morphed to show him addressing the troops while wearing a pink ballerina's tutu, and his ruling council rose up against him in embarrassment and disgust, the action would be perfectly legal—and somewhat amusing.

Effect of Hostilities on International Obligations. The legal analysis for information operations becomes most complex in the peacetime legal regime, where many acts permissible in war are violative of international law. It is therefore vital to ascertain the effect of armed conflict on that peacetime regime.

The first step is to determine if the treaty in question has a specific termination or suspension clause. If it does not, then the object and purpose of the treaty controls whether or not it applies in wartime—only those obligations inconsistent with a state of hostilities fall out. Belligerents must still respect the rights of neutral parties to a multilateral treaty. The nature of some information operations, as relatively peaceful steps short of armed conflict, makes their intended use in a pre-wartime environment very attractive for policymakers. For those operations comprising simple intelligence collection, the lack of an international prohibition of espionage leaves decisionmakers with the usually acceptable liability of merely violating the target nation's domestic espionage law. However, information operations that do more than gather information, but actually have real-world consequences, may violate more than just the adversary's domestic law. Short of actual belligerency, information operations implicate the range of legal issues outlined above.

Application. Unusual targets and unusual means for reaching them are the hallmark of information operations. But no matter how subtle or complex the fact pattern, according to John Norton Moore, "there's *always* a right answer."[69] In this case, the right answer can be reached by applying the basic principles of proportionality, discrimination, and chivalry to each new target. Whether or not these individual operations will be carried out in the context of the *jus in bello* is most clearly determined by applying Pictet's criteria to the larger conflict.

For example, if the operation is being undertaken as part of a larger military effort in an acknowledged war, the Pictet analysis is not necessary. Assume the target is an electronic funds transfer from the dictator of an adversary nation to his account in the Cayman Islands. The opposing country may attempt to corrupt the transmission as it passes through a certain communications satellite. Assuming the technology to do this exists, the military necessity of manipulating the transfer (perhaps reducing it from $198,000 to $1.98) would be balanced against whatever unnecessary suffering such an act may produce. The military necessity may arise from using such an attack to convince the dictator that his most valued assets are at risk, and thus specifically deter him

from prosecuting the war any further. Unnecessary suffering, in this case, would not outweigh military necessity, because beyond the dictator and his immediate circle of retailers, such suffering would probably be *de minimis*.

The principle of discrimination is satisfied because the weapon and the target are not proscribed, and because the attack is tightly focused on the enemy leader, presumptively the senior member of his military's operational chain of command. In wartime, this is sufficient to render an enemy dictator a lawful target. In peacetime, the question is somewhat less clear, where an action below the Article 2(4) threshold could still run afoul of the target country's domestic criminal law. However, this is the peacetime norm for espionage and covert operations, and this information operation does not present any fundamentally new legal features.

The final step would be an examination of the act's chivalry. In our example, the act appears not to be perfidious. The law of war does not cover economic attacks, so no dictator could reasonably expect legal protection beyond any applicable national criminal laws. In addition, the transfer was not induced, but merely attacked, by the U.S. Therefore, it appears that such an attack would be lawful.

Conclusion

What, then, are the specific steps to follow in performing a legal analysis of offensive information operations in space? First, correctly identify the type and subtype of operation contemplated. The three types are intelligence collection, offensive operations *through* satellites, and offensive operations *against* satellites. The subtypes for each are listed in the second section of this paper.

Second, determine if this type of operation, in the light of all relevant circumstances, rises to the level of a use of force. Although international legal academics are only now turning to this question, the one settled concept in this area is that an information operation crosses the Article 2(4) threshold when it produces effects comparable to those of a kinetic attack which would be thought of as having crossed the threshold. What more than that would constitute a use of force is still an open question.

If the action is the equivalent of a use of force, it may only be undertaken pursuant to Chapter VII authorization, or as a lawful exercise of self-defense. Assuming the legality of acting at all, the operation must be conducted in accordance with the customary international legal standards of proportionality, discrimination, and chivalry.

Offensive information operations in space will drive a revolution in technical, tactical, and legal thought. It is for the attorney adviser to the warfighter to present honest, closely reasoned legal advice to his client so that he may fight honorably and effectively.

NOTES

* Counsel and Senior Policy Analyst, AEGISResearch Corporation, Falls Church, Virginia. The opinions and conclusions expressed here are those of the author and do not necessarily reflect the views of any governmental or private entity.

1. DEPARTMENT OF DEFENSE DIRECTIVE S-3600.1, INFORMATION OPERATIONS (IO), December 9, 1996.
2. Bruce Wald & Gary Federici, *Commission on Roles and Missions of the Armed Forces: Defending the Civilian Information Infrastructure—Does DoD Have a Role*?, CIM 417, (Center for Naval Analyses, Alexandria, VA), May 1995, at 1.
3. JOINT CHIEFS OF STAFF JOINT PUBLICATION 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS, Oct. 9, 1998, at I-3 [hereinafter JOINT PUBLICATION 3-13].
4. Captain Sir Basil Liddel Hart, *Thoughts on War*, 1944, *quoted in* JOINT PUBLICATION 3-13, *see id.*, at II-7.
5. JOINT PUBLICATION 3-13, *supra* note 3, at GL-4.
6. The taxonomy which follows is the author's own, but employs unclassified terms of art familiar throughout the intelligence community.
7. Attitude movement attacks may also be mounted by "bumping" a target satellite with another satellite, or even by latching on and firing the attack satellite's thrusters.

8. U.N. CHARTER art. 2, para 4.
9. *Id.* at art. 51.
10. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 187 (2d ed. 1994).
11. *See supra* note 8, at art. 39.
12. *See supra* note 8, at chapter VII.
13. *See supra* note 8, at art. 41.
14. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205.
15. *Id.*
16. *Id.* at art. I.
17. *Id.* at art. III.
18. *Id.* at art. IV.
19. *Id.* at art. VI.
20. *Id.* at art. VII.
21. *Id.* at art. XI.
22. *Id.* at art. XII.
23. Convention on International Liability for Damage Caused by Space Objects, March 29, 1972, 24 U.S.T. 2389, T.I.A.S. No. 7762.
24. *Id.* at art. II.
25. *Id.* at art. III.
26. *Id.* at art. VI.
27. *Id.* at art. VIII and IX.
28. *Id.* at art. X.
29. *Id.* at art. IX.
30. Agreement Relating to the International Telecommunications Satellite Organization, Aug. 20, 1971, 23 U.S.T. 3813, T.I.A.S. No. 7532.
31. *Id.* at art. I.
32. *Id.* at art. I, ¶ (k).
33. *Id.* at art. 1, ¶ (l).
34. *Id.* at art. III, ¶ (d).
35. *Id.* at art. III, ¶ (e).
36. Convention at the International Maritime Satellite Organization, Sept. 3, 1976, 31 U.S.T. 1, T.I.A.S. No. 9605.
37. *Id.* at art 3(3).
38. International Telecommunication Convention, with Annexes and Protocols, Nov. 6, 1982, art. 19, __ U.S.T.__, T.I.A.S. No. ___, Senate Treaty Document 99-6.
39. *Id.* at art. 19.
40. *Id.* at art. 20.
41. *Id.* at art. 35.
42. *Id.* at art. 38.
43. *Id.* at Annex 2.
44. Treaty on the Limitation of Anti-Ballistic Missile Systems, May 26, 1972, art. XII, 23 U.S.T. 3435, T.I.A.S. No. 7503.
45. Walter Gary Sharp, Sr., *Cyberspace and the Use of Force: Information Warfare, the Law of War, and the United States Standing Rules of Engagement*, Legal Aspects of Information Warfare Symposium, (1995).
46. 47 U.S.C. § 502.
47. 18 U.S.C. § 1367.
48. UNITED STATES COMMANDER-IN-CHIEF, ATLANTIC (USCINCLANT) MEMORANDUM 5800 J20L, *Legal Aspects of Offensive Information Warfare – Information Memorandum*, 1 (Jan. 16, 1996).
49. DEPARTMENT OF DEFENSE DIRECTIVE 3600.1, INFORMATION OPERATIONS (IO), Dec. 9, 1996.
50. JOINT CHIEFS OF STAFF INSTRUCTION, CJCSI S-3210.01A, JOINT OPERATIONS WARFARE POLICY, Jan. 2, 1996 (Classified Secret; no classified sections are referenced).

51. DEPARTMENT OF DEFENSE INSTRUCTION 5000.1, INFORMATION OPERATIONS (IO), DEFENSE ACQUISITION, March 15, 1996.
52. DEPARTMENT OF DEFENSE DIRECTIVE 5100.77, July 10, 1979.
53. U.N. CHARTER art. 2, para 4.
54. Collectively, these conventions are referred to as the four Geneva Conventions of 1949, which are as follows: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31, *reprinted in* Adam Roberts and Richard Guelff, DOCUMENTS OF THE LAWS OF WAR 171 [hereinafter LAWS OF WAR]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85, *reprinted in* LAWS OF WAR 194; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, *reprinted in* LAWS OF WAR 216; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287, *reprinted in* LAWS OF WAR 272.
55. COMMENTARY OF THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 583 (Jean S. Pictet ed., 1958).
56. OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE ARMY, INTERNATIONAL AND OPERATIONAL LAW HANDBOOK 18-2 (1995) [hereinafter OPERATIONAL LAW HANDBOOK]. *See also* U.S. ARMY FIELD MANUAL 27-10, ¶ 41.
57. Professor Sharp makes this point very clearly in his new text:

> The principle of proportionality is frequently misunderstood as limiting the use of force that can be used to destroy a military objective to the strength or firepower of that objective – or in some other way limiting the use of force between combatants. It does not, however, require any such parity of force. Proportionality is a limitation on the use of force against a military objective only to the extent that such a use of force may cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians. The principle of proportionality is a balancing of the need to attack a military with the collateral damage and human suffering that will be caused to civilian property and civilians by the attack. Categorically, proportionality imposes *no* limitations on the use of force between combatants in the absence of any potential effects on civilians or civilian property.

WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 40 (1999).
58. OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, ¶ 5.2 (1989).
59. *Id.* at ¶ 5.2.
60. Colonel Phillip A. Johnson, Associate Deputy General Counsel (International Affairs) in the Office of the General Counsel, Department of Defense, presentation at Annual Review of the ABA Standing Committee on Law and National Security, 1996.
61. OPERATIONAL LAW HANDBOOK, *supra* note 56, at 18-1.
62. Regulations Respecting the Laws and Customs of War on Land, annexed to the Hague Convention No. IV Respecting the Laws and Customs of War on Land, Art. 53 [hereinafter HAGUE REGULATIONS].
63. DEPARTMENT OF THE NAVY, OFFICE OF THE CHIEF OF NAVAL OPERATIONS, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 5-1, NWP 1-14M (Oct. 1995).
64. Final Report to Congress on the Conduct of the Persian Gulf War, April, 1992, Appendix O, 4-106.
65. HAGUE REGULATIONS, *supra* note 62, art. 24.
66. Protocol Additional to the Geneva Conventions of 12 August, 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977, 1125 U.N.T.S. 3, art. 37(2), [hereinafter Protocol I].
67. AIR FORCE PAMPHLET 110-31, INTERNATIONAL LAW—THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, § 8-4(a).
68. Protocol I, *supra* note 66, art. 37(1).
69. John Norton Moore, Lecture at Georgetown University Law Center (July 13, 1995).