Counterspace Operations for Information Dominance

Before discussing offensive counterspace operations in support of information dominance, an understanding of the strategic objectives of an information dominance strategy is needed.

Strategic Objectives

Information dominance should be thought of as a condition in which a nation possesses a high degree of understanding of an adversary's military, political, social, and economic strengths, and weaknesses, interdependencies, and centers of gravity while denying the same information to the adversary.[1] Military actions directed against the enemy should be undertaken with the strategic objective of delaying, disrupting, and denying information that could be used by enemy leadership to effectively execute military strategy. The objective is to convince the enemy that he cannot execute his military strategy successfully. Therefore, the strategic center of gravity in an information dominance strategy is the enemy leaders, both military and civilian, who rely on information to execute the national military strategy. In essence, the endgame is to increase their uncertainty regarding their ability to successfully execute military strategy.

In future warfare, space systems will be the strategic and tactical eyes and ears of a national security establishment. Therefore, controlling space is essential to achieving information dominance. In an information dominance strategy, however, the objectives of space control must be viewed in a different context. Currently, the objective of space control, as outlined in Air Force doctrine is to gain supremacy or control over the environment of space. Historically, this objective has tended to focus offensive counterspace operations on destroying satellites in space. On the other hand, space control under an information dominance strategy seeks control over the information or products that space systems provide. An objective of this nature recognizes that space systems are distributed weapon systems,

consisting of three segments: an orbital segment, a ground segment, and a link segment that connects the orbital and ground segments and disseminates the information to military and civilian leadership.[2] Control of space systems information can be accomplished through attacks against any of these segments—and control does not necessarily involve the physical destruction of equipment or facilities. The operational objective of offensive counterspace operations for information dominance, therefore, is to delay or deny an enemy's capability to collect, process, and disseminate information by disrupting or destroying the enemy's space systems.

Operational Concept

Since information dominance can create uncertainty regarding the focus and thrust of the theater campaign, offensive counterspace operations should normally precede other theater operations. To attain information dominance, offensive counterspace operations should use a combination of lethal and nonlethal weapon systems to attack the operational center of gravity of a space system. Depending on the space system, the enemy, and the level of conflict, the center of gravity can be located in any of the three segments of an enemy's space system.

Different nations have different levels of space capabilities, which we refer to as segments. For discussion purposes, we propose three levels:

- Tier-one nations have ground segments, link segments, and orbital segments.
- Tier-two nations have ground segments and link segments.
- Tier-three nations have ground segments only.

Operational centers of gravity in the orbital segment of an enemy's space system can be the entire satellite or the satellite subsystems that are critical for mission performance. A satellite does not have to be destroyed to prevent it from accomplishing its mission; damaging or disrupting vital satellite subsystems can prevent the satellite from effectively accomplishing its mission. Examples of vital subsystems

include satellite attitude control sensors, mission sensors, uplink/downlink antennas, and power generation systems.

The center of gravity in the link segment is the communications link, the radio frequency used to pass information to and from the satellite. Since most satellites rely on uplinked command and control information from the ground for station keeping, payload management, and satellite health and status functions, attacking a satellite's uplink during critical commanding periods could seriously degrade mission performance. The effectiveness of electronic jamming, however, is limited due to line-of-sight restrictions and increased satellite autonomy; therefore, attacking the downlink, rather than the uplink, is usually easier and more reliable in disrupting a space system. Since the satellite downlink telemetry contains the mission information and health and status information on the spacecraft and the satellite's sensor, successfully attacking the downlink directly attacks information flow and, therefore, has a more immediate effect on achieving information dominance.

The centers of gravity in the ground segment include satellite launch facilities, command and control facilities, and processing stations (airborne, seabased, fixed or mobile landbased). All parts of the ground segment are vulnerable to attack from clandestine operations, air attack, and direct ground attack.

Weapons for Offensive Counterspace Operations

What type of technology is needed to conduct offensive counterspace operations for information dominance? Historically, doctrine and policy addressing space control has focused primarily on hard-kill technologies to destroy orbiting satellites. Other technologies, however, can be used to achieve offensive counterspace objectives without physical destruction of the orbiting satellite. Nondestructive soft-kill (e.g., mission-kill) technologies can permanently disable the satellite without destruction, while nonlethal technologies can be used to achieve nonpermanent space system mission degradation and disruption. The specific technologies used for offensive counterspace

operations can be grouped according to the segment they are targeted against: orbital, link, or ground.

Offensive counterspace weapons used to attack the orbital segment of a space system usually fall into one of two technology categories: kinetic energy or directed energy.

Kinetic energy is a hard-kill technology that causes physical destruction of the orbiting satellite. Weapons based on kinetic energy employ projectiles that can be launched into space to destroy orbiting satellites through the shock of impact. There are three types of kinetic energy antisatellite (ASAT) weapons: exploding fragmentary warheads, guided nonexplosive warheads that collide with satellites, and space mines. The benefit of using a kinetic energy ASAT weapon is the high probability of denying all information from the attacked satellite. The disadvantages include a lack of plausible deniability regarding the reason the satellite failed and the identity of the attacker.

Perhaps the most flexible of the technologies used for offensive counterspace weapons is directed energy. Directed-energy weapons can be employed to achieve a destructive hard kill, a nondestructive soft kill, or a nonlethal temporary disruption or degradation. Examples of directed-energy weapons are lasers and high-power microwave weapons. Lasers use electromagnetic radiation (light) for either lethal or nonlethal attacks on satellites.[3] Depending on their power, lasers can damage, disrupt, or destroy a satellite by overheating its surface, puncturing the outer surface of the spacecraft to expose internal equipment, or blinding critical onboard mission or control sensors.[4] Ground-based lasers, such as the Russian laser at Sary Shagan, are estimated to have a satellite hard-kill capability up to 400 km and a soft-kill capability up to 1,200 km.[5]

Another directed-energy technology that can be used for offensive counterspace operations is high-power microwave. High-power microwave weapons employ radio frequencies to damage satellite electronics. Unlike kinetic energy and some types of laser attacks, high-power microwave weapons achieve satellite subsystem failure rather than vehicle failure.[6] Intelligence estimates suggest it is possible to construct a microwave radiation weapon today with a

satellite soft-kill capability of about 500 km. In addition, microwave radiation at lower power levels can be effectively used for satellite jamming.[7] Using directed-energy weapons against the orbital segment in an offensive counterspace operation has several advantages. First, since directed-energy attacks take place at the speed of light, they are near instantaneous, thereby minimizing the effectiveness of enemy defenses. Second, there is plausible deniability associated with soft kill and nonlethal satellite attacks. The adversary may not have the capability to detect the nature or the source of the attack, or even whether a hostile action actually occurred. Hence, plausible deniability can be useful in politically sensitive situations. Third, the desired results can be tailored from nonpermanent disruption and degradation to permanent degradation and destruction.

The link segment, as mentioned earlier, consists of the electromagnetic energy used for space system uplink, downlink, and in some cases a crosslink. Given that the link segment is made up of electromagnetic energy, the primary technology used to attack the link segment is electronic warfare. There are two ways to use electronic warfare to attack the link segment: jamming and spoofing. Jamming consists essentially of transmitting a high-power, bogus electronic signal that causes the bit error rate in the satellite's uplink or downlink signals to increase, resulting in the satellite or ground station receiver losing lock.[8]

Attacking the link segment by spoofing involves taking over the space system by appearing as an authorized user, such as establishing a command link with an enemy satellite and sending anomalous commands to degrade its performance.[9] Spoofing is one of the most discrete and deniable nonlethal methods available for offensive counterspace operations.[10]

Offensive counterspace operations directed against the ground segment include all offensive actions directed against a satellite launch complex, command and control facilities, and ground processing stations. The ground segment is vulnerable to all types of terrestrial attacks, from special operations to strategic attack with gravity bombs. While the ground segment is the most vulnerable

segment in a space system, it may also represent the higher political and military risk. Typically, ground segments for space systems are distributed within the enemy's homeland to reduce single point failures and to reduce their vulnerability to attack. In addition, high development costs associated with dedicated military space systems and rapidly advancing commercial technology possessing inherent military utility have resulted in an increase of dual use (military/civilian) space systems. Therefore, in many tier-two and tier-three space-capable nations, ground segment targets are usually located near urban areas susceptible to collateral damage and civilian casualties. Although all forms of direct attack can be used, it may be more politically acceptable and less militarily risky to attack ground segment targets with highly accurate precision munitions.

In the final analysis, the available technologies for conducting offensive counterspace operations appear to be flexible and responsive. We must remember, however, that the employment options are situation-dependent.

Offensive Counterspace Options

The biggest drawback of our current offensive counterspace strategy is that there are some conflict situations in which destroying an enemy's satellite with an ASAT is not an attractive or realistic option. However, in an information dominance strategy, the objective is to delay or deny information; therefore, employment options for offensive counterspace operations can exist for all threat nations at all conflict levels against all segments of a space system.

Employment options for conducting offensive counterspace operations in an information dominance strategy are influenced by three major variables: the threat (e.g., tier one, two, or three), the level of conflict (e.g., peace, crisis, or war), and the segment of the space systems to be attacked (orbital, link, or ground). Depending on the threat and the level of conflict, employment options for offensive counterspace operations applicable to the three segments of a space system can range from "no option" at the low end of the spectrum to

ASAT attack against the satellite or strategic attack against the ground station at the high end of the spectrum. Although an information dominance strategy provides our military planners greater flexibility for conducting counterspace operations, examination of potential offensive counterspace employment options reveals that offensive counterspace operations are shaped by two trends.

One trend is that different segments of a space system become subject to attack and the level of acceptable violence increases as the level of conflict moves from peace to war. During a crisis, for example, the orbital segment could be attacked with nonlethal disruption weapons; during war, the orbital segment could be attacked by either hard- or soft-kill mechanisms.

The second trend is that as the threat from space decreases, the threshold for attacking space systems increases and the level of acceptable violence decreases. In no case is attacking an orbital segment of a tier-three nation with hard- and soft-kill mechanisms viewed as being politically acceptable, whereas it would be against a tier-one nation.

The ability to delay and/or deny information from space systems at all levels of conflict permits the establishment of information dominance during peacetime and its sustainment through crisis and war. Determining options for offensive counterspace operations for information dominance can be illustrated in the following scenario. The potential for a crisis exists between the US and a tier-three nation that has a licensed *satellite pour l'observation de la terre* (SPOT) ground station. If a crisis erupts, the US, wanting to be prepared with a rapid show of force in the theater of operations, issues a warning order to preposition forces. To ensure secrecy, the theater commander requests offensive counterspace operations to deny the enemy nation information from the SPOT system that could reveal the force mobilization. The only available option for offensive counterspace operations during peacetime is electronic warfare against the link segment. If the situation escalates to war, the options for counterspace operations will expand. Eventually, those options will span all

segments of the space system and encompass the entire spectrum of violence, from nonlethal soft kill to lethal soft kill to lethal hard kill.

Summary

Information dominance strategy as an alternative to the current space control strategy has three advantages. First, because the strategy focuses on the denial of information rather than denial of the environment, the link and ground segments of the space system correctly reemerge with an increased relevance to offensive counterspace operations. This total systems approach has essentially increased the operational flexibility of offensive counterspace operations by increasing the operational centers of gravity that can be targeted. Second, the total systems approach, coupled with a philosophy that satellite destruction is no longer essential, has resulted in an increase of available technologies for offensive counterspace operations. Options for employing existing capabilities, such as nonlethal directed energy, electronic countermeasures, and precision-guided munitions, seem more politically viable than the destructive ASAT, which in the past has been questioned by many within Congress. Finally, the increased number of space system targets subject to attack, coupled with the ability to employ a broader assortment of lethal and nonlethal technologies, creates options for employing offensive counterspace operations across the spectrum of conflict.

Notes

1. Lt Col Andrew F. Krepinevich, Jr., *The Military Technical Revolution, A Preliminary Assessment* (Washington, D.C.: Office of the Secretary of Defense and Office of Net Assessment), 8.

2. Paul B. Stares, *Space and National Security* (Washington, D.C.: Brookings Institution, 1987), 74.

3. lbid.,75.

4. Ibid.,76.

5. Cmdr James S. Green, *U.S. Plan for Space Control* (Maxwell AFB, Ala.: Air War College, 3 March 1989), 7.

6. Ralph Zirkland, *Evaluation of Soviet Exploitation of CM/CCM in Space Warfare* (U) (McLean, Va.: Defense Technical Information Center, Defense Logistics Agency, November 1983). (Secret) Information extracted is unclassified.

7. Maj William O'Dell, *Application of Electronic Countermeasures in the Defense of U.S. Space Object* (U) (Maxwell AFB, Ala.: Air Command and Staff College, May 1973). (Secret) Information extracted is unclassified.

8. *Electronic Warfare Threat to U.S. Communication Links (T-J)* (U) (Washington, D.C.: Defense Intelligence Agency). (Secret) Information extracted is unclassified.

9. Ibid.

10. Stares, 82.