



ANNEX 3-14 SPACE OPERATIONS

DEFENSIVE SPACE CONTROL

Last Updated: 19 June 2012

Potential adversaries have access to capabilities that can deceive, deny, disrupt, degrade, or destroy US [space capabilities](#). Defensive space control (DSC) operations preserve US and friendly abilities to exploit [space](#) to their advantage via passive and active actions to protect friendly space-related capabilities from enemy attack or interference.

DSC operations provide the means to deter and defend against attacks and to continue operations by limiting the effectiveness of hostile action against US [space assets and forces](#). DSC operations include [deterrence](#) of attacks against our [space systems](#), defense of our space systems as they come under attack, and where necessary, recovery of our space forces and assets. Given the distributed nature of space systems, a variety of forces and assets are employed to deter, defend, and recover our space capabilities from attack. Deterrence, with an emphasis on a demonstrated national policy of appropriate response to threats or attacks and the national will to respond to such threats or attacks, remains at the forefront of protection of our space system assets and forces. If deterrence fails, defense of US and friendly space capabilities from deception, denial, disruption, degradation, or destruction by an adversary is crucial to maintain space superiority. While many defensive measures are passive in nature, the ability to detect and characterize an attack on friendly space capabilities is critical for the initiation of most active measures.

The United States' space advantage is threatened by the growth in adversary counterspace capability and the adversary's increased use of space. In the past, the United States enjoyed space superiority through our technology development and exploitation, advanced information systems, and robust space infrastructure. The ability to sustain this advantage is challenging and may be eroding as our adversaries close the gap through technology sharing, materiel acquisition, and purchase of space services. Adversaries can conduct attacks against our space capabilities using multiple methods. Adversaries may have the capacity to develop counterspace capabilities or, in many cases, may simply acquire them from a third party.

Near and long-term [threats](#) include the following:

- ✦ Ground system attack and sabotage against terrestrial nodes and supporting infrastructure.
- ✦ [Electromagnetic jamming](#) equipment capable of interfering with space system links.

- ✦ Laser systems able to temporarily or permanently degrade or destroy satellite subsystems.
- ✦ Electromagnetic pulse weapons capable of degrading or destroying satellite and/or ground system electronics.
- ✦ Kinetic anti-satellite (ASAT) weapons capable of destroying spacecraft or degrading their capabilities. Direct ascent systems are best visualized as being “surface-to-space missiles,” while orbital ASAT systems are also possible.
- ✦ Computer offensive cyberspace operations capabilities which can corrupt space-based and terrestrial-based computer systems used to control satellite functions and to collect, process, and disseminate mission data.

Adversaries do not need to be space-faring nations to exploit the benefits of space. Adversaries can purchase space products and services, such as imagery and communications, which may rival those available to US military forces. Adversaries may leverage US or friendly systems to their advantage as well. For example, an adversary may use the Global Positioning System (GPS) constellation for navigation. Adversary access to space decreases US advantage and increases the threat to friendly military forces.

DSC Passive Measures

DSC passive measures deter and mitigate adversary attacks against US and friendly space systems. Passive measures enhance the survivability of space systems by providing a layered defense to ensure critical space systems continue to operate both during and after attack. Known survivability measures may even deter an adversary from attempting to attack our space systems. Passive measures include the use of: camouflage, concealment, and deception (CC&D); hardening of systems; dispersal; redundancy; information assurance (IA); and operations security (OPSEC). All of these DSC passive measures are discussed below except for redundancy, which is covered later in the DSC section on recovery operations.

Camouflage, Concealment, and Deception. CC&D is most effective with terrestrial-based nodes. Certain types of ground-based components of space systems may operate under camouflage or be concealed within larger structures. These measures complicate adversary identification and targeting.

System Hardening. Hardening of space system links and nodes allow them to operate through attacks. Electromagnetic hardening techniques such as filtering, shielding, and spread spectrum help to protect capabilities from radiation and electromagnetic pulse. Physical hardening of structures mitigates the impact of kinetic effects but is generally more applicable to ground-based facilities than to space-based systems due to launch-weight considerations. Robust networks, aided by redundancy and the ability to reroute, ensure operation during and after information operations attack.

Dispersal of Space Systems. For space nodes, dispersal could involve deploying satellites into various orbital altitudes and planes. For terrestrial nodes, dispersal could involve deploying mobile ground stations to new locations. Dispersal not only applies to passive measures but also to active measures, as discussed in the DSC active measures section on maneuver/mobility later in this chapter.

Information Assurance. [Information Assurance](#) (IA) protects and defends information within our network of space systems. IA measures to prevent compromise of information include encryption and authentication of command links and encryption of data generated onboard space platforms. As with system hardening, IA measures include filtering, shielding, and spread spectrum techniques to prevent denial of information from electromagnetic jamming or interference.

Operations Security. OPSEC protects our space operations from compromise by reducing adversary access to critical information about our space forces and capabilities and indicators of activity.

DSC Attack Detection and Characterization

Effective attack detection and characterization rely on robust space situational awareness. Detecting and characterizing an adversary's attack on space systems and assessing the impact of these attacks enable DSC active measures and provide post-attack indications and warning for other space forces.

Detection. The process of attack detection confirms that a space system is under attack. The ability to quickly and accurately distinguish between hostile, unintentional, and natural events is critical to the ability to detect attacks on space systems. Without such confirmation, DSC active measures should not be undertaken. Given today's capabilities, attack detection involves the support of multiple organizations.

Characterization. Identifying the nature of the attack and the type of attack system facilitates locating the attacker and initiating COAs in response. Ideally, analysis should take place as close to the tactical level as possible, thus decreasing the amount of time between detection and identification. Analysis may often take time due to coordination between organizations involved, the need for certainty, and technological limitations. Detailed analysis may require the support of non-Air Force DOD agencies as well as non-DOD entities.

Impact Assessment. Impact assessment begins when an attack is detected. It provides an understanding of the effect an attack is having on the targeted asset, associated systems, and services provided. Accurate assessment is important, as it provides a basis for determining an appropriate response.

Location. The location of an attacker must be known to actively suppress an attack. Various support capabilities must be brought in synergistically to provide a geographic location and confirmation.

DSC Active Measures

Active measures for DSC may involve actions to avoid or remove hostile effects. Physical adjustments to the nodes and links of space systems, such as a maneuver or frequency change, may avoid hostile effects. Use of conventional or special operations forces may stop an adversary's counterspace attack. The key to these active measures is early detection and characterization of the threat in order to determine the most effective countermeasure.

Maneuver/Mobility. Satellites may be capable of maneuvering in orbit to deny the adversary the opportunity to track and target them. They may be repositioned to avoid directed energy attacks, electromagnetic jamming, or kinetic attacks from ASATs. Today, maneuver capability is limited by on-board fuel constraints, orbital mechanics, and advanced warning of an impending attack. Furthermore, repositioning satellites generally degrades or interrupts their mission. The use of mobile terrestrial nodes complicates adversarial attempts to locate and target command and mission data processing centers. However, movement of these nodes may also impact the system's capability, as they must still retain line of sight with their associated space-based systems. Though the use of mobile technology is expanding, many of today's ground-based systems are not mobile, making physical security measures essential.

System Configuration Changes. Space-based and terrestrial nodes may use different modes of operation to enhance survivability against attacks. Examples include changing radio frequency (RF) amplitude and employing frequency-hopping techniques to complicate jamming and encrypting data to prevent exploitation by unauthorized users.

Suppression of Adversary Counterspace Capabilities. Suppression of adversary counterspace capabilities (SACC) neutralizes or negates an adversary offensive counterspace system through deception, denial, disruption, degradation, and/or destruction. SACC operations can target air, land, maritime, space, special operations, or information operations in response to an attack or threat of attack. Examples of SACC operations include (but are not limited to) attacks against adversary anti-satellite weapons (before, during, or after employment), intercept of anti-satellite systems, and destruction of electromagnetic jammers or laser blinders.

DSC Recovery Operations

Recovery operations focus on restoring a disrupted space capability. Two techniques that apply to recovery operations are redundancy and reconstitution.

Redundancy. Redundancy may be incorporated into space-based or terrestrial capabilities, or within a link itself. Redundancy in equipment components allows continued operations of specific platforms in the event of onboard hardware or software malfunction. Systems may have redundancy through the use of on-orbit satellite spares or use of alternate commanding, tracking, and relay stations. Link redundancy can be achieved through the use of alternate frequencies for command or mission information along with data multiplexing techniques.

Reconstitution. Reconstitution involves actions to restore operations after an attack. It may also involve repairing equipment that has been degraded or deploying new space and terrestrial platforms to replace combat losses. Reconstitution of satellite constellations requires responsive spacelift, available replacement spacecraft, and properly trained personnel to launch and operate the systems.

DSC Resources and Forces

The following are some of the forces and weapon systems that could be used, if and when available, to support DSC operations.

Physical security systems provide security and [force protection](#) for critical ground facilities and equipment. A complementary mix of technology and security forces can effectively and efficiently mitigate specific threats in an ever-changing environment. When properly deployed and utilized, physical security systems can represent an effective deterrent and provide aggressive defense against terrestrial node attack and sabotage.

Air defense assets are capable of protecting launch and terrestrial nodes from air or missile attack. If threatened, commanders should consider deploying air defense assets such as aircraft, surface-to-air missiles, and/or anti-aircraft artillery to protect critical space assets (e.g., facilities and infrastructure). A sound air defense may deter an adversary and most certainly will be instrumental in defending our forces and assets if an attack is attempted.

Attack detection and characterization systems detect space system attacks and provide information on the characteristics of the attack, especially if the source and/or capability of the attack is unknown or unexpected. These systems will support locating the source of the attack and the type of weapon used in the attack. They may be ground-, air- or space-based and either integrated with systems they protect or used in a stand-alone capacity. Having our adversaries aware of these capabilities may act as an effective deterrent and influence their decision.

Conventional and special operations forces may conduct defensive space control operations through their ability to attack adversary counterspace capabilities. A demonstrated capability and willingness to counter their space capabilities may deter an adversary from attacking US/friendly space capabilities.
