EXECUTION CONSIDERATIONS

Last Updated: 25 January 2021

The Commander, United States Space Command (CDRUSSPACECOM) executes operations based on global requirements for national defense and requests from multiple theaters. Space forces are continuously employed and executing. This requires timely deconfliction and integration with theater operations. The Combined Space Operations Center (CSPOC) integrates space operations on behalf of the CDRUSSPACECOM through a deliberate coordination process with the applicable theater air operations centers.

The effectiveness of counterspace operations depends on the availability and capability of specific resources and systems. System capabilities are influenced by the situation, threats, weather, and available intelligence. In all cases, planners should consider the use of multi-domain capabilities to conduct counterspace operations. The following are some of the resources and capabilities that may be used to conduct offensive counterspace (OCS) and active defensive counterspace (DCS) operations:

- **Aircraft.** Aircraft can be used to provide effects in support of OCS operations. For instance, by attacking ground stations with either electronic attack or kinetic weapons, aircraft may negate an adversary's ability to control their satellites and deliver space effects.

- **Surface Forces.** Surface forces may include conventional land, maritime forces, or special operations forces (SOF). Surface forces can achieve significant effects through the lethality of surface fires and the ability to occupy and secure key areas. For example, surface forces may attack a ground-based satellite control station in support of OCS operations. SOF may provide terminal guidance for conventional air strikes or provide localized jamming against an adversary's link segment.

- **Electromagnetic Warfare.** Electromagnetic warfare may be used to suppress enemy command and control (C2), integrated air defense systems, and other significant military use of the electromagnetic spectrum. Electromagnetic warfare weapons may include electromagnetic jammers and anti-radiation missiles. Jammers may be used to interfere with adversary link segments. Anti-radiation missiles passively hone in on a radiation source and may be used to strike ground-based space surveillance radars or satellite control stations. See AFDP 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*, for detailed discussion of all aspects of electronmagnetic warfare.

- **Information Operations and Cyberspace Operations.** Information operations and

cyberspace operations can greatly enhance joint operations. All three segments of an adversary space system may be affected by offensive cyberspace operations. Some techniques afford access to targets that may be affected by information operations and cyberspace operations in support of OCS operations.

- **Anti-Satellite Weapons**. Anti-satellite (ASAT) weapons include direct ascent and orbital systems that employ various tactics to affect or destroy on-orbit satellites or spacecraft.
- **Missiles.** These weapons include surface-to-surface, air-to-surface, and air-to-air missiles, as well as air-, land-, and sea-launched cruise missiles. Many of these weapons have long ranges and some have very quick reaction times. Missiles may be employed against an array of adversary ground segment targets, such as launch facilities and ground stations.
- **Directed Energy Weapons.** Directed energy weapons, such as lasers, may be land-, maritime-, air-, or space-based. Depending on the power level used, directed energy weapons could be capable of a wide range of effects against on-orbit satellites, including: heating, blinding optics, degradation, and destruction. Under certain circumstances, lasers could also be effective against space launch vehicles while in flight.

The targets for counterspace operations may include the adversary space, ground, or link segments. The space segment includes satellites and other spacecraft. The ground segment includes land-based, maritime-based, or airborne equipment and resources used to deploy, enable, or use space capabilities. The link segment connects the space and ground segments and enables the passing of information between them. Understanding that space capabilities are a combination of these segments increases the operational planners' ability to choose the correct target and the best ways and means to affect adversary space capability. The following paragraphs discuss examples of counterspace targets.

- **Space Segment.** Satellites are on-orbit assets consisting of a payload and a satellite bus. The payload performs the operational function of the satellite. The satellite bus hosts the payload and provides it with power, thermal control, and communications. Counterspace operations may target the payload and/or the satellite bus. For example, a laser may deny, disrupt, degrade, or destroy certain types of sensors. Kinetic ASAT weapons, on the other hand, may target the satellite bus to achieve physical destruction.
- **Ground Segment.** The ground segment may perform many functions, including satellite operations, counterspace operations, mission data processing, C2, or launch functions. The ground segment may consist of permanent structures that represent a single point of failure in a space system. However, space operations may also be conducted from mobile or deployable terrestrial platforms. Launch facilities, whether indigenous or third party, are critical for access to space and represent a critical node for interdicting efforts to augment or reconstitute adversary space capabilities.
- **Link Segment.** Space systems are dependent on radio frequency (RF) and/or laser links to provide communication between the space and ground segments (satellite-to-ground station or satellite-to-user) and between satellites (satellite-to-satellite). Links between terrestrial nodes may include fiber-optic and traditional cable in addition to RF and laser links. On-orbit satellites and ground-based satellite control stations users exchange data across the link segment. The up-link may contain satellite commands used to task satellite payloads and buses. The down-link is used for sending payload and satellite telemetry data to a ground stations for processing. The ground station, after

processing the mission data, often distributes this data to users via satellite communications (SATCOM) for exploitation. In the case of SATCOM systems, data may be directly up-linked and down-linked between users.

- **C2 Systems.** C2 capabilities are critical to the effective employment of forces and should be given a high priority during targeting. Countering C2 systems substantially reduces the enemy's capability to detect, defend, and attack friendly forces in all domains.
- **Third-Party Providers.** An adversary may gain significant space capability by leveraging third-party space systems. Leveraging diplomatic or economic means to remove an adversary's access to third-party (commercial or foreign) space capabilities will generally require the support of other US Government departments.

Active Defense

Active defense includes any direct actions taken in response to an attack against friendly space forces, assets, or capabilities, as well as actions taken in response to unintentional or environmental threats. These actions include:

- **Movement and Maneuver.** Satellites may be capable of maneuvering in orbit to deny the adversary the opportunity to track and target them. Maneuver capability is limited by on-board fuel constraints, orbital mechanics, and the time taken to plan and execute a maneuver. Furthermore, repositioning of 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 as well as deployable space capabilities. However, movement of these ground segment nodes may also impact the system's capability, as they must still retain line of sight with their associated space segment. Movement and maneuver in the link segment may include actions such as changing frequencies, shifting users to other satellites (whether commercial or military), and moving spot beams or altering beam shape. Movement and maneuver can also exploit alternate communications paths like fiber or theater communication architectures, such as line-of-sight or airborne relay.

- **System Configuration Changes.** Satellites and ground segment nodes may use different modes of operation in the link segment to enhance survivability against attacks. Examples include changing RF amplitude and power to complicate jamming.

- **Suppression.** Suppression of adversary threats to friendly space capabilities negates or mitigates the effects of those threats through deception, denial, disruption, degradation, or destruction. These operations may be conducted by friendly capabilities in any domain to negate adversary threats originating in any domain in response to a threat.

Passive Defense

Unlike active space defense measures, passive space defense does not involve direct action in response to adversary, unintentional, or environmental threats. Passive defense includes the following measures:

- **Camouflage, Concealment, and Deception**. Certain 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 allows them to operate through attacks and environmental threats. 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.
- **Cybersecurity**. Cybersecurity protects and defends information within our network of space systems. Cybersecurity measures to prevent compromise of information include encryption and authentication of command links and encryption of communications signals. As with system hardening, cybersecurity measures include filtering, shielding, and spread spectrum techniques to prevent denial of information from electromagnetic jamming or interference.
