CURTIS E. LEMAY CENTER
FOR DOCTRINE DEVELOPMENT AND EDUCATION

AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-14
COUNTERSPACE OPERATIONS

THREATS TO SPACE OPERATIONS

Last Updated: 25 January 2021

Potential adversaries see increasing value in the ability to attack US and allied space capabilities. Adversaries may employ multiple means, developed organically or acquired from third parties. Near- and long-term threats include the following:

- **Terrestrial Attack.** Kinetic attack or sabotage against terrestrial nodes and supporting infrastructure. Examples of terrestrial nodes include operations centers, command and control nodes, and communications relays.

- **Electromagnetic Attack (EA).** Electromagnetic (EM) energy used to attack a link segment, to include uplink, downlink, and crosslink signals.

- **Directed Energy (DE).** Directed-energy threats include laser, radio frequency (RF), and particle-beam weapons. Laser systems may be used to temporarily disrupt or deny capabilities or to permanently degrade or destroy satellite subsystems. RF weapons concepts include ground and space-based RF emitters that fire high-power bursts of EM energy at a satellite, imparting disruptive EM fields into the wiring and electrical components in order to upset and possibly damage the computer processing subsystems. Particle-beam weapons could be used to fire beams of charged particles at a satellite, superheating and destroying structural materials and mission components.

- **High Altitude Nuclear Detonation.** A nuclear explosion can potentially affect all three segments of several space systems at the same time. Since the effects of nuclear detonation move out rapidly and permeate all space, no satellites have to be targeted directly. An electromagnetic pulse will induce damaging voltages and currents into unprotected electronic circuits and components of affected satellites and terrestrial nodes. The radiation generated by the detonation could damage satellite components and shorten their effective operational lives from years to days.

- **Anti-Satellite (ASAT) Weapons.** Weapons capable of destroying or degrading spacecraft and spacecraft components and/or denying or disrupting their capabilities. There are two basic types. Direct ascent systems are best visualized as being “surface-to-space missiles,” while on-orbit ASAT systems are also possible. ASATs may cause structural damage by impacting the target. Even small projectiles can inflict substantial damage or destroy a satellite. More advanced ASAT weapons could employ proximity operations and robotic arms to seize target satellites or use stand-off capabilities such as EA and DE.

- **Offensive Cyberspace Operations.** Cyberspace attacks may disrupt or deny space-based or terrestrial-based computing functions used to conduct or support satellite operations and to collect, process, and disseminate mission data.

- **Environment**. Neutral and environmental threats include weather, space debris, and unintentional EM interference. While not intended to do harm, this category of neutral and environmental threats causes increasing concern due to the potential impact to space operations.

- **Weather**. Just as weather affects air operations, space and terrestrial weather can impact satellites, their communications links, and ground segments. For example, solar storms can have a direct impact on the functioning and survivability of satellites, while thunderstorms and cloud cover may impact the functionality of the ground and link segments.

- **Debris**. The space domain is becoming more congested with active satellites and debris. This congestion increases the satellite collision probability, which could damage satellites and even result in additional debris. The resulting debris would likely continue to accumulate and congest the most valuable orbits for the foreseeable future.

- **Electromagnetic Interference**. The demand placed on the electromagnetic spectrum continues to grow as the number of satellites, satellite services, and users increases. Increased congestion limits the available spectrum and increases the potential for unintentional interference on friendly signals. To complicate the issue further, international spectrum management practices create uncertainty in gaining access to the required spectrum and impose strict limitations on power, bandwidth, and coverage.