FACT SHEET: Resilience of Space Capabilities

As we invest in next generation space capabilities and fill gaps in current capabilities, we will include resilience as a key criterion in evaluating alternative architectures.

National Security Space Strategy

The National Security Space Strategy (NSSS) charts a path for the next decade to to maintain and enhance the advantages derived from space while confronting the challenges of an evolving space environment. The NSSS seeks to address a strategic space environment that is increasingly congested with increasing amounts of space debris; contested by a growing range of foreign counterspace capabilities; and competitive as more and more countries and companies operate in space. Resilience is one way to address this more challenging space environment. The strategy notes that strengthening the resilience of our architectures can deny the benefits of an attack on our space infrastructrure, as well as enable our ability to operate in a degraded space environment.

Key Ideas Underpinning Resilience

The purpose of resilience is to assure performance of military and related intelligence functions at a level necessary to execute assigned missions within an acceptable tolerance for risk. This functional mission assurance must account for the full range of anticipated scenarios, conditions, and threats that drive our planning. Combatant Commanders largely define "acceptable risk" for military functions in consultation with the Secretary of Defense, Director of National Intelligence, and Commander in Chief.

We primarily seek to make resilient the military functions dominantly provided by space systems. Thus, the focus is on traditional missions that support the warfighter, as well as the underlying missions required to conduct space operations.

Resilience is comprised by capabilities from multiple domains. Therefore, resilience is evaluated at the enterprise, mission, or functional level in a manner that encompasses the systems and system of systems provided by multiple domains that enable a given function. The evaluation of resilience must also comprehend the contributions of capabilities within a domain.

Resilience to both hostile actions and adverse conditions is needed. Therefore, resilience must equally consider threat-based hostile acts, as well as aberrations caused by any number of natural or man-made adversities.

Resilience focuses on maintaining or replenishing capabilities, and thus transcends conventional risk mitigation efforts. Risk management and mitigation initiatives primarily focus on reducing threats to components and systems. By focusing on sustaining critical capabilities, resilience shifts thinking from the protection of key assets to the sustainment of key capabilities and the maintenance of the functional enablers that support these capabilities.

We must strike a balance between risk-based functional performance, resilience, and affordability. Resilience may not always require increased investment. Changes in policy, practice, or procedure can offer real operational value. Cost sharing with allies, as well as leveraging commercial hosting opportunities, can add performance and resilience.

Resilience encompasses avoidance, robustness, reconstitution, and recovery

- ***Avoidance:*** countermeasures against potential adversaries, proactive and reactive defensive measures taken to diminish the likelihood and consequence of hostile acts or adverse conditions
- ***Robustness:*** architectural properties and system of systems design features to enhance survivability and resist functional degradation
- ***Reconstitution:*** plans and operations to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency
- ***Recovery:*** program execution and space support operations to re-establish full operational capability and capacity for the full range of missions, operations, or contingencies

Definition

Resilience is the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.

Levels of Evaluation

Resilience can be measured at multiple levels. The primary measure of resilience at the Enterprise, Mission, and Functional levels is risk to national security objectives, mission effectiveness, or functional capability. Resilience is also assessed at the Domain, Constellation, and individual Space System level.

Criteria for Evaluation

The five evaluation criteria below provide a common measure to assess resilience for any given functional architecture.

1. Anticipated ***level of adversity***
2. ***Functional capability goals*** necessary to support the mission
3. The ***risk*** that these goals may not be met at a given level of adversity
4. The ***severity*** of the functional shortfall to the mission
5. The ***time*** which the shortfall can be tolerated by the mission

The temporal component of this evaluation construct is of particular import. Time primarily quantifies the reconstitution component of resilience. Restoral is presumed to be a more lengthy replacement effort tied to more traditional planning and programmatic activities that extend well past the period of crises.

Next Steps

This resilience definition and criteria can form a basis from which to institutionalize resilience into our architectures, requirements, planning, programming, acquisition, and operations activities. Resilience is essential to assure our functional capabilities, particularly those enabled by space, at a time when the domain is increasingly congested, contested, and competitive.