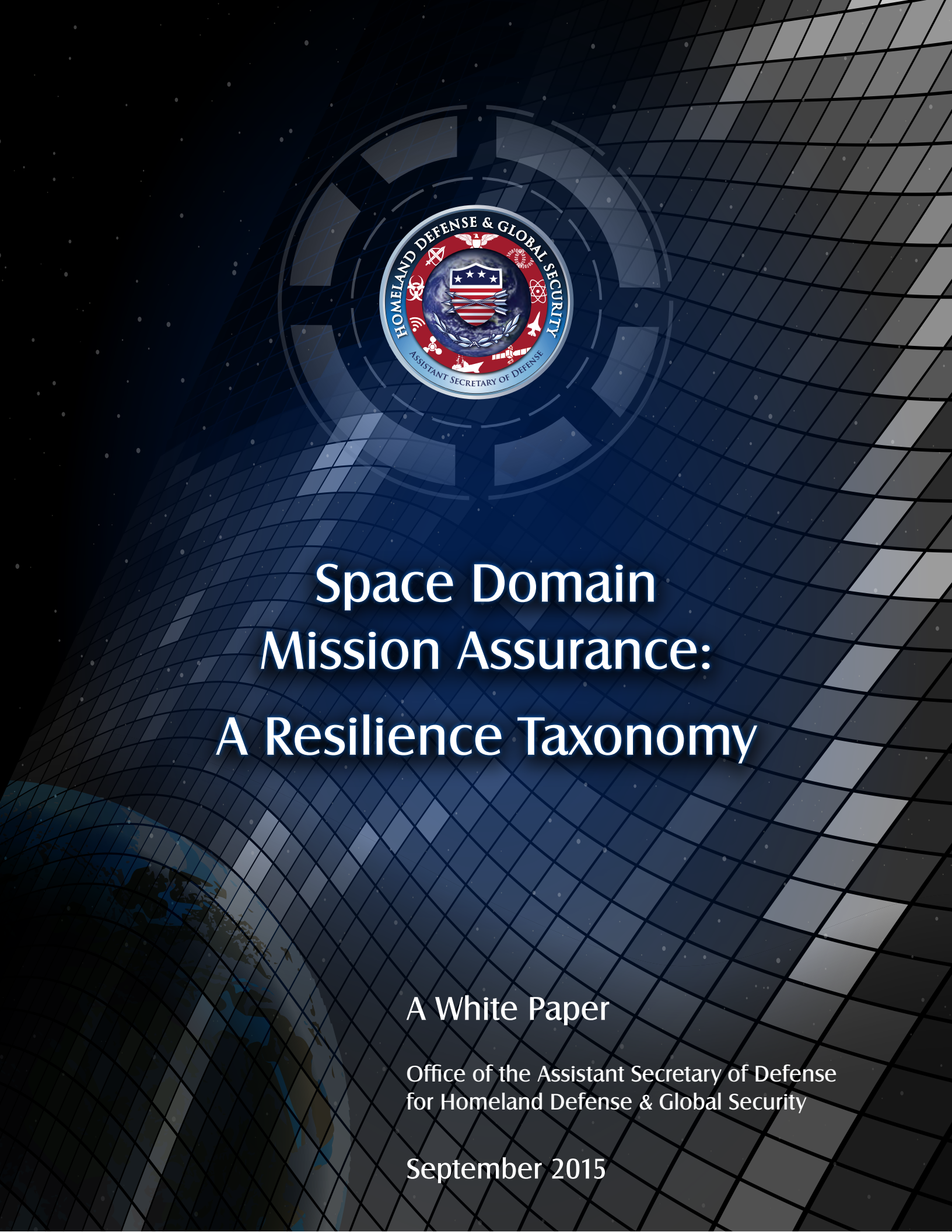


Space Domain Mission Assurance: A Resilience Taxonomy

A White Paper

Office of the Assistant Secretary of Defense
for Homeland Defense & Global Security

September 2015

Background

Today's space architectures, designed and deployed under conditions more reflective of nuclear warfighting deterrence than conventional warfighting sustainability, lack, in general, the robustness that would normally be considered mandatory in such vital warfighting services. In recent years, overcoming this lack of robustness has been summed up in a single term, *resilience*.

National and Departmental level guidance call for bolstering resilience and making resilience a consideration in all architectural planning and evaluation, as well as in all system planning and development activities for DoD space capabilities. The 2011 US National Security Space Strategy directs the National Security Space community to, "strengthen the **resilience** of our architectures to deny [adversaries] the benefits of an attack (emphasis added)."[1] This followed the guidance in the 2010 National Space Policy to "[e]nsure cost-effective survivability of space capabilities, including supporting information systems and networks, commensurate with their planned use, the consequences of lost or degraded capability, the threat, and the availability of other means to perform the mission."[2] Flowing from the guidance of the National Space Policy and the National Security Space Strategy, the 2012 DoD Space Policy Directive (DoDD 3100.10) calls for considering reliability, protection, and resilience of required space capabilities in all architecture planning and evaluation. DoDD 3100.10 also calls for consideration of risks and threats, consequences of loss, and the availability of alternatives for mission accomplishment to be included in all system planning and development activities for defense space capabilities.

Unfortunately, the National Security Space community lacks both an agreed-upon taxonomy for discussing resilience, and a quantitative method for measuring it. As such, conversations on possible alternatives for future space system architectures and deployment strategies stumble, and eventually degenerate into either cost-driven or capability-driven comparisons of various futures, leaving resilience as an afterthought. That is not to say that neither cost or capability should be driving issues – they should. But one can argue that the costliest and least capable space system is the one that is not available when the fighting is underway and it is needed the most. Therefore, resilience must exist at the forefront of any space planning or architecture analysis, and, as such, we must reach agreement on what that means.

Purpose

The purpose of this paper is to define the OSD Policy perspective of a viable taxonomy for space mission assurance, and its conceptual origin. It is beyond the scope of this paper to discuss measurement techniques – that is a job for engineers and system developers. However, the quantification job becomes more practical, and the conversation of alternatives more understandable, once the taxonomy is established and agreed upon. That is not to declare that

[1] National Security Space Strategy (Unclassified Summary), Jan 2011, pg. 10
[2] National Space Policy of the United States of America, June 28, 2010, pg. 13

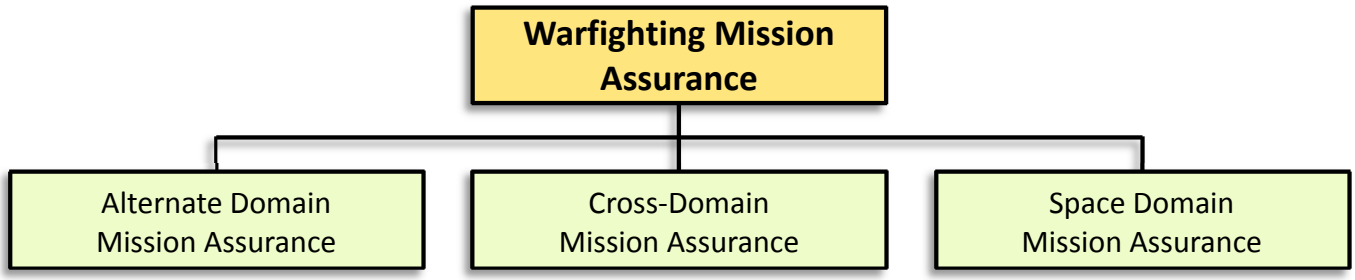
there is only one possible taxonomy; indeed there are many. But as long as the selected taxonomy encompasses all concepts with unique categories for each type of approach, then it provides a sufficient conceptual framework for analysis.

In this resilience taxonomy, we chose to expand the subject to one of ***warfighting mission assurance***.[3] The April 2012 DoD Mission Assurance Strategy defined mission assurance as "A process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD mission essential functions in any operating environment or condition." Resilience is not the end which we seek to assure; it is the warfighting mission assurance benefit, derived from resilience, which we seek to assure.

Approach

Conceptually, we elected to examine mission assurance from a domain-related perspective – alternative domain mission assurance (which in this case would mean non-space), multi-domain or "cross-domain" mission assurance (combining space and non-space domains), and in-domain (space only) mission assurance. This domain-related approach is shown below in Figure 1.

Figure 1: Warfighting Mission Assurance



For the purposes of this paper, we then begin to expand the foundations of in-domain or space-related mission assurance, remembering that there will be added contributions to overall warfighting mission assurance from alternative or cross-domain solutions as well.[4]

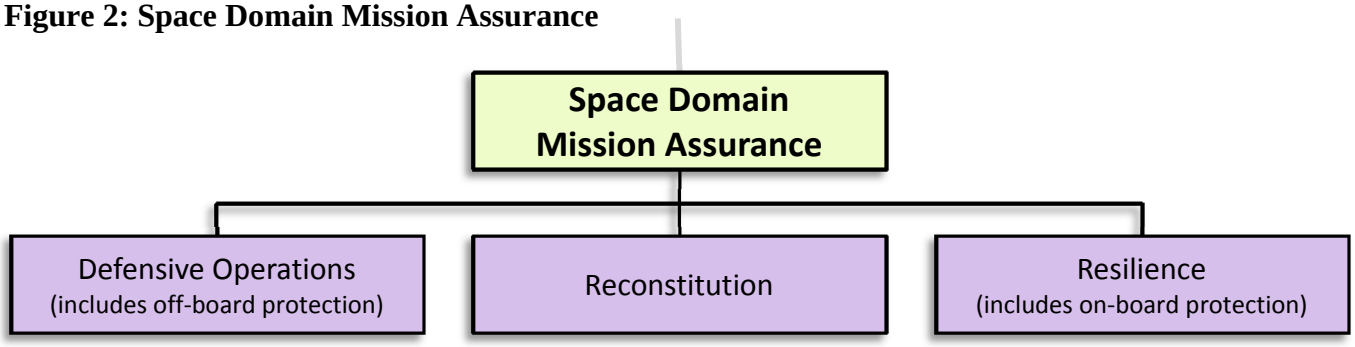
As we next examined different organizational systems for understanding space domain mission assurance, we sought to satisfy ourselves that all possible means for providing that

[3] The term "mission assurance" is often used in talking about space systems from an engineering/technical standpoint. Those treatments of mission assurance are not the subject of this discussion, which is concerned with warfighting continuity, not engineering sufficiency.

[4] In a complete discussion of warfighting mission assurance, each of the other domains would have its own particular foundational taxonomy. This paper only examines the space-related branch of that taxonomy. It is also unclear whether cross-domain resilience simply reduces to the sum of the resilience in the alternate domain and the space domain, but, at least for now, we chose to maintain it as a separate item in the taxonomy.

assurance were included in the resulting categorization. We considered all plausible methods of assuring that the space mission continued in the face of adversary action or environmental stresses, and that each of those methods had a "home" within the mission assurance categories. We also sought to ensure that the taxonomy included modalities associated with the non-space elements (telemetry, tracking, and command nodes, spectrum utilization, etc.) of the space capability. We ended up adopting three basic conceptual approaches for mission assurance; (1) Defensive Operations (which includes off-board protection elements), (2) Reconstitution, and (3) Resilience (which includes on-board protection elements) (see Figure 2).

Figure 2: Space Domain Mission Assurance



While these three approaches are interrelated, and in some cases have overlapping subordinate elements, they seemed to provide adequate separation and complete coverage of the overall area. We defined each according to either published or well-understood descriptions of their qualities:

Defensive Operations: *Activities or operations undertaken to interrupt an adversary kill chain, or provide warning or insight to the targeted mission system in support of defensive actions.*[5]

Reconstitution: *Plans or operations to bring new assets on line (e.g. launching replacement satellites or activating new ground stations) in order to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency after an attack or catastrophic event.*[5]

Resilience: *The ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions […].*[6]

[5] Definition for the purpose of this white paper
[6] As defined in DoDD 3100.10

It is worth noting that in charting the derivation of the word "resilience" as followed in this taxonomy, some qualities or approaches that have been included in other resilience discussions are specifically excluded. The prime example here would be the pursuit of alternate or cross-domain solutions, such as air solutions, to provide space system resilience. We argue that such alternate or cross-domain approaches do aid in the greater goal of assuring the warfighting mission, but they do not meet the goal of actually increasing the resilience of the space architecture itself. This is no different than in other areas of warfare where we might seek, for example, to bolster the resilience of the long range bombing force by the use of stealth or hypersonic vehicles, while at the same time we pursue a non-aircraft based, missile focused, prompt global strike capability. Few would argue that the missile system bolsters the resilience of the bomber force, but it does contribute to assuring the mission of global reach. Similarly, we have separated reconstitution and defensive operations from resilience. Both contribute to the ultimate goal of providing space domain mission assurance, but they do not directly support the resilience of the space system.[7]

Defensive Operations

Defensive operations reduce the likelihood that an adversary will be able to mount a successful attack on our space architectures, and, to a certain extent, are independent of the space mission defended. This type of capability or operation might include disrupting the adversary's ability to target space systems or directly intercepting an attacking system. Thus, synchronized and systematic maneuvers of on-orbit assets to confuse and overwhelm an adversary's targeting system and active measures to deceive, degrade or destroy targeting systems would all be examples of "defensive operations." Defensive operations also include the necessary friendly SOSI capability needed to provide warning of and to characterize the attack and blue force command and control (C^2) capabilities to execute the defense. It is easy to see that such capabilities represent a "tide that raises all ships" and therefore, we believe, are better left segregated from specific system resilience discussions.

Reconstitution

The second approach is reconstitution; launching additional satellites or bringing additional ground stations, new signals and spectrum into play to bolster the ability to provide the capabilities and capacity required for mission success. This is not the same as recovery, which Webster's defines as "bringing back to a normal position or condition; to save from loss and restore to usefulness." Recovery involves restoring the utility of our remaining assets to the maximum extent possible. Reconstitution involves adding back capability or capacity through additional assets or links.

[7] We recognize that this segregation is somewhat arbitrary, but we believe that by following this path we can provide better focus to the ultimate question of how to improve the resilience of specific system architectures even as we seek to take other (reconstitution, defensive) steps to assure the space mission.

In some ways, reconstitution can offset a resilience requirement; the more quickly you can reconstitute your space capabilities, the less resilient those capabilities need to be on their own (assuming your reliance upon those capabilities is held constant). The reverse is also true; the less quickly you can reconstitute a given space capability, the greater your need for those capabilities to be inherently resilient. Resilience and reconstitution complement one another. In a similar manner as defensive operations, many reconstitution approaches tend to have applicability across a variety of mission areas. It is also true that the ability to reconstitute a given space capability is strongly affected by the architectural choices made with respect to that space capability from the earliest stages of conception. One could choose to emphasize reconstitution as a factor when making architectural decisions[8], but even if one maximized the ability to reconstitute a given space capability, that would merely mitigate, not eliminate, the need for resilience with respect to that space capability. So we find that resilience and reconstitution can be traded to meet a certain mission assurance requirement, and therefore rightfully deserve segregation, in a well-formulated taxonomy.

Resilience

This brings us to resilience, which we define as an internally-focused characteristic of an architecture. This is contrasted with reconstitution and defensive operations, which are external to the architecture, though architectural decisions would affect the ability to reconstitute that architecture or employ defensive operations to defend it.

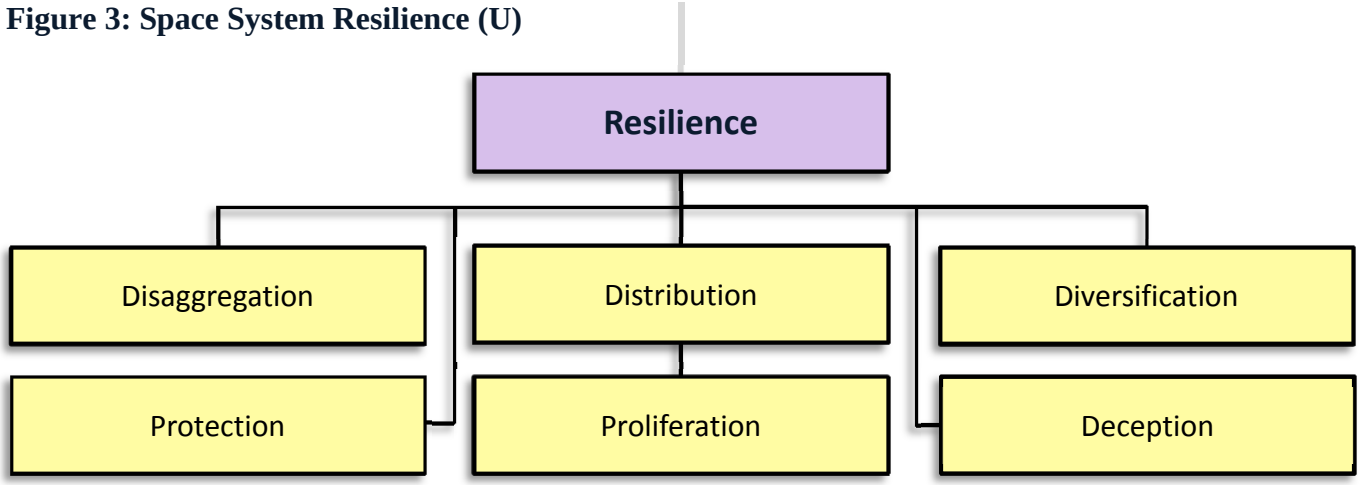
We have treated resilience, reconstitution, and defensive operations separately because we believe that this is better-ordered intellectually. In addition, and perhaps more importantly, we recognize how these distinctions relate to the Department's decision-making with respect to fielding space capabilities. If resilience is spread out across multiple internal and external elements of an architecture or if resilience is the sum of qualities that are fielded around a capability, as well as within a capability, then it is difficult, if not impossible, to determine who is responsible for that capability's resilience. It becomes extremely difficult to characterize that resilience in a closed form analysis, and it becomes nearly impossible to develop a quantitative method for measuring and comparing resilience across alternative future system architectures. In short, more expansive formulations of resilience lead to the results we discussed at the outset: decisions that devolve into the cost-capability trade-offs that are so familiar. Put another way, resilience becomes someone else's problem—we just can't tell you whose problem it is. But as an internal quality, resilience now squarely becomes the capability designer's problem, and becomes tradable with other system characteristics.[9]

[8] For example, an imaging architecture based on small, numerous, and quickly deployable and operable imagers is more easily reconstituted than an architecture of large, sparsely numbered, and delayed-operability systems. For the former, you may choose to emphasize reconstitution vice resiliency; versus the later, where resiliency becomes more important.

[9] It is important to note that in eventual resource decisions, all three of these space domain mission assurance approaches must be traded—they complement one another in assuring that the ultimate warfighting capability can be

We applied the same approach to developing the sub-elements of resilience as we did for the sub-elements of space domain mission assurance. We looked at multiple means of achieving resilience from all the sources that had examined this problem, and then tried to develop the fewest categories into which they could be sufficiently organized. We arrived at six discrete characteristics to describe resilience approaches: disaggregation, distribution, diversification, protection, proliferation, and deception (see Figure 3).

Figure 3: Space System Resilience (U)



Disaggregation

Disaggregation is defined as the separation of dissimilar capabilities into separate platforms or payloads. An example of this would be separating tactical and strategic protected satellite communications. It should be noted that disaggregation may serve, and be justified by, a variety of purposes that are worthy in and of themselves, but which may not relate to resilience. Separating tactical and strategic protected satellite communications, for example, may help mitigate the risk of uncontrolled escalation during a crisis or conflict without necessarily bolstering resilience. Further, disaggregation can also apply in other cases to reduce the complexity of systems, making it easier to implement other resilience characteristics. In this respect, disaggregation is a means to an end; not bolstering resilience directly, but allowing it to occur more readily.

Distribution

Distribution is defined as utilizing a number of nodes, working together, to perform the same mission or functions as a single node. For example, the Global Positioning System (GPS) is a distributed system. No individual satellite, or ground monitoring site for that matter, is

---

delivered through space. But those trades are best made within the resourcing process, not the system analysis process.

fundamental to assuring positioning, navigation, and timing (PNT) in any one specific location. Losing a single node, satellite or ground station, begins to reduce the accuracy of the system, and with enough losses, the availability of the system. But the highly resilient nature of the GPS architecture, a byproduct of its distributed design, allows for more graceful degradation and presents an adversary with an expanded target set with a far larger number of targets than if the system relied on a singular node. It is also worth noting that GPS satellites and monitoring stations are individually fairly inexpensive, allowing this distribution to be applied more widely and changing the cost calculus for an adversary.

Diversification

Diversification is defined as contributing to the same mission in multiple ways, using different platforms, different orbits, or systems and capabilities of commercial, civil, or international partners. Systems or architectures that are flexible or adaptable for use in support of a variety of mission sets are also examples of diversification. Using PNT again as an example, the diverse nature of space-based PNT systems can be used to assure that warfighters have access to at least one space-based PNT capability, even if a primary means is denied.[10] A similar dynamic arises for other systems with vast commercial and international participation (communication and ISR). As we will see for other elements of resilience, diversification coupled with other approaches (proliferation and deception) can be used to create resilient architectures. And since diversification also presages the use of alternative, non-U.S.-government systems, it can increase resilience with lower investments than some other techniques.

Protection

Protection is defined as active and passive measures to ensure those U.S. space systems, and those of our partners upon which we rely, provide the required quantity and quality of mission support in any operating environment or condition. This includes traditional steps we have taken such as jam protection and nuclear hardening, and can be extended to maneuverability, internally hosted decoys, and other on-board countermeasures. It could also include efforts within the system to better characterize and attribute effects of adversaries (these have been termed "self-awareness" in some studies) to enable satellite operators to restore functions, capabilities, or capacity after a natural or man-made adverse event.

Proliferation

Proliferation is defined as deploying larger numbers of the same platforms, payloads or systems of the same types to perform the same mission. For example, deploying a larger number

[10] By 2020 the assessment is that there will be over 140 individual PNT satellites in orbit through constellations such as GPS, Galileo, QZSS, IRNSS, EGNOS, GAGNOS, Beidou, GLONASS, WAAS, and others. This is a highly diversified space capability. These systems each have independent monitoring stations, control nodes, frequencies of operation, and integrity monitoring systems.

of Wideband Global Satellite Communication (WGS) satellites in the WGS constellation, or by increasing the number of downlink and data processing facilities. Here again, the resilience benefits of such efforts could be magnified if proliferation efforts were coupled with other complementary resilience measures. For example, proliferation could be joined with diversification and protection through use of commercial systems that complement and provide alternatives to military satellite communications, and through development of protected tactical waveforms for communications on those commercial systems.

Deception

Deception is a longstanding practice by which commanders hide both their strengths and weaknesses from their adversaries. They use deception to cloak their intent and achieve operational and strategic surprise. Similarly, commanders of space national security assets must consider deception in their planning for space operations to ensure the survival and resilience of their space mission.

We define deception as measures taken to confuse or mislead an adversary with respect to the location, capability, operational status, mission type, and/or robustness of a national security system or payload. While many deception measures could be taken at the system level, such as constructing different payloads or components in a manner that would make them difficult to distinguish from others that perform different functions, there are deception measures one could take at an architectural, operational, or organizational level as well. To the degree that deception measures are successful, an adversary either: (a) will not attack a given space system or capability that he would attack if he realized what and where it was or the actual function it performed; or (b) may be induced to attack systems that do not provide the capabilities that he is attempting to degrade. Given the physics of space defense and attack, deception is likely a critical element of any space system resilience effort.

Summary

As we have noted previously, all of these resilience measures, along with reconstitution and defensive measures, and alternate/cross domain abilities may be used individually and collectively to achieve warfighting mission assurance. Resilience is but one contributor to that equation. But we believe it is a critical component to define at the system level, in the control of the system designer, analyst, and operational commander to help drive those requirements that cannot be addressed through resilience alone.

The National Space Policy, the National Security Space Strategy, and DoDD 3100.10 require that space mission assurance and resilience be included in space system planning. This taxonomy is an appropriate basis for that planning and should be used to address these policy requirements.


HOMELAND DEFENSE & GLOBAL SECURITY
ASSISTANT SECRETARY OF DEFENSE