SPACE AGENDA 2021

GETTING THE MOST DETERRENT VALUE FROM U.S. SPACE FORCES

Michael P. Gleason and Peter L. Hays

As space becomes more crowded and contested it becomes ever more important to prevent a conflict in, directed toward, or from space. Without any actual experience of combat in space, however, we can only speculate about what role the space domain might play in a breakdown of deterrence and the start of a war. This inexperience with space's role in conflict complicates social science's already limited understanding of how wars begin and unfold—with their complex interplay of political goals, differing levels of commitment, the friction generated in any actual fighting, and the inherently flawed people (on all sides) making decisions. As the strategic environment changes, we must explore ways to strengthen the contribution of U.S. military space capabilities to deterrence while also enhance any advantages should deterrence fail. Focusing on the credibility of U.S. space capabilities in some narrow areas reveals steps that could be made to strengthen their deterrent value.

Background

Russian and Chinese efforts to field antisatellite (ASAT) weapons represent serious threats to U.S. national security and complicate U.S. deterrence efforts. According to the U.S. Defense Intelligence Agency (DIA), China's People's Liberation Army (PLA) already has operational ground-based ASAT weapons to destroy satellites in low Earth orbit (LEO), and the PLA has military units dedicated and trained to use them. In addition, China may already have a limited capability to use laser systems against satellite sensors, will likely deploy a ground-based laser weapon operationally before the end of 2020, and within the next ten years may have lasers powerful enough to damage satellites themselves, not only satellite sensors.[1] China is also developing advanced on-orbit capabilities which could serve as inspection and repair satellites or co-orbital weapons. Dedicated counterspace electronic warfare and jamming weapons also threaten U.S. space capabilities and cyber-attacks are a threat in space, just like in other domains.[*] While reflecting different priorities and investment decisions, Russian efforts generally mirror Chinese development of counterspace weapons.

The vulnerability of U.S. military, intelligence, and partner satellites to these threats weakens the United States' conventional deterrence abilities and potentially undermines the U.S. nuclear deterrent. Conventionally, Russia and China see their space attack capabilities as a means to level the battlefield with the U.S. military. U.S. military and intelligence satellites, as well as the commercial satellites the U.S. military uses, are critical to the modern American way of war. But if

[*]For a more detailed discussion see *A Roadmap for Assessing Space Weapons*, also from CSPS.

those satellites can be destroyed or at least disrupted, Russian and Chinese terrestrial forces may perceive a narrower disadvantage and those nations may be more willing to start a war.

U.S. space capabilities enable U.S. nuclear deterrence strategy by gathering and delivering intelligence on adversaries' nuclear weapons dispositions, verifying Russian compliance with nuclear arms control agreements, providing the United States with warning of a nuclear attack, and providing U.S. decision-makers with tight command and control of U.S. nuclear forces. If attacking those satellite capabilities is perceived as a way to prevent the United States from responding to a nuclear attack, nuclear deterrence may be undermined. Moreover, even if the adversary attacks U.S. satellites only in pursuit of limited, regional objectives, the United States may perceive itself to be under strategic attack.

Worryingly, space is perceived as an offensive dominant arena, meaning it is considered materially easier and less costly to *attack* a satellite than to *defend* a satellite. Political scientists contend that war is more likely when the offensive is dominant—especially if it is difficult to distinguish between offensive and defensive weapons as is the case with space—and they argue that there are strong incentives for striking first should a conflict appear inevitable.[2] Surprise attack is perceived as leading to large rewards, fueling a first-mover advantage for striking in space. But the speed with which events can happen in space leads to the potential for crisis instability since decisionmakers—on all sides—will have very little time (perhaps only a few minutes) to decide what to do in the face of a sudden attack in space. In short, perceived weaknesses in the ability of space forces to protect themselves can lead to a broader breakdown in deterrence.

An exploration of deterrence theory fundamentals can serve as a guide on how to mitigate some of these weaknesses and strengthen the deterrence value of U.S. military space capabilities while contributing to achieving advantage should deterrence fail.

Fundamentals

Deterrence is a psychological concept intended to prevent undesired behavior and activity. As detailed in the study of nuclear deterrence, there must be at least two actors in the deterrence calculus and there are two basic approaches: deterrence by punishment and deterrence by denial.[3] Each approach emphasizes different concepts of operations and favors different capabilities and architectures. An integrated approach is ideal, but trades between the two approaches make a fully integrated approach difficult. Punishment attempts to deter undesired behavior by credibly threatening to punish assailants with overwhelming force or other punitive action in retaliation for an aggression. The punishment need not be in the same domain or region as the initial attack; it may not even need to be a military response. The December 2017 *National Security Strategy of the United States of America* sends a deterrence by punishment message where it states:

> The United States considers unfettered access to and freedom to operate in space to be a vital interest. Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing.

Under this threat, actors may be deterred from undesired behavior if they conclude that the costs of the behavior outweigh the benefits. Denial, by contrast, attempts to deter undesired behavior by leading actors to conclude that they will be unable to achieve the objectives they seek from their behavior. Denial requires effectively responding in the same time and place as the attack.

To prevent a breakdown in deterrence, both punishment and denial require that the actor attempting to deter undesired behavior is perceived as possessing needed capabilities, is credible in exercising those capabilities under threat of counter-retaliation and potential escalation, and has successfully communicated its capabilities and credibility to the actors it intends to deter.

Table 1: Requirements for One Actor to Deter Another Actor
Be perceived as possessing required capabilities
Be perceived as credible in exercising those capabilities and in possessing the willingness to suffer counter-retaliation and escalation
Be able to successfully communicate capabilities and credibility to those being deterred

The study of deterrence reveals many complexities and nuances associated with the *concept* of deterrence which could lead to a breakdown in *actual* deterrence, including:

- Differing perceptions of undesired behavior, rationality, and credibility
- Divergent ways different cultures allocate values to cost-benefit analyses
- Philosophical differences in understanding causation

These are not addressed here so the focus can remain on the issues particular to deterrence in the space domain and how a breakdown in general deterrence may follow several paths flowing from these peculiarities. Demonstrating the credibility of U.S. capabilities is at the core of the issue and is key to getting the most deterrent value from U.S. space forces.

The Credibility of U.S. Attribution of Attacks in Space

To deter, the United States must be able to attribute an attack on its satellites. Attribution refers to the ability to determine the actor(s) responsible for creating certain effects and, in many space scenarios, can be difficult to determine. Space has a wide range of naturally occurring phenomena such as micro meteoroids and geomagnetic storms which can interfere with satellite operations in ways that can be hard to distinguish from interference intentionally caused by human actions. We also have limited fidelity about many ongoing space activities, satellite systems, and their orbital locations. Moreover, the amount of and dangers posed by debris continue to grow and pose problems. Accounting for the effects of debris that is too small to track but still large enough to damage or disable a satellite presents one of the most daunting attribution challenges. Finally, many space capabilities can be used for military, civil, and commercial purposes. These growing dual-use entanglements make it difficult to identify individual space actors or single uses of space capabilities, complicating attribution and leading to several potential paths to a broader breakdown in deterrence.

A key challenge for strategists is to identify ways for the United States to demonstrate its capability to attribute malicious behavior in space in light of these problems. The adversary should perceive that it will be caught.

Table 2: Attribution Difficulties in Space
Distinguishing natural phenomenon from intentional interference
Limited fidelity about space activities and sensor limitations
Space debris that is too small to track but still can cause damage
Dual-use entanglements

A *deterrence by punishment* strategy has more stringent attribution requirements. To justify a punitive response elsewhere, an actor must have defensible evidence of what happened that it is willing to share with allies and the public. If an adversary is confident that its responsibility for an attack may be obscured or unattributable—quite possible in space with all the attribution difficulties noted above— the adversary may calculate that it can avoid retaliation for the attack and get away with a *fait accompli*. Therefore, for deterrence by punishment to be most credible, the adversary must perceive that it will *not* be able to escape responsibility for an attack in space due to the United States' inadequate ability to confidently attribute the attack.

Table 3: Attribution, Punishment, and Space
Possess the most stringent attribution requirements
Shape an adversary's perception of the United States' capability to confidently attribute an attack
Have the need to share some amount of attribution information to get domestic political/allied support for retaliation
Have the need to reveal, to some degree, U.S. decisionmaking processes for retaliation

However, an adversary's mere *perception* of attribution is not sufficient. Since conflict escalation might need broad support from American opinion leaders and the public as well as support from allies and commercial partners, attribution information likely needs to be credible and available to share with this broad range of stakeholders.

If the United States decides to emphasize a deterrence by punishment strategy for attacks on its space assets, it will have to communicate, to some extent, its criteria and decisionmaking processes for deciding to retaliate. The United States provides such insights about its nuclear deterrence strategy in the public release of how information on a nuclear attack warning flows to the president, about how much time the president has to make a decision, and how the president gives the command to retaliate. But the United States, by necessity, also must keep some aspects of its nuclear capability secret to ensure it is effective; if too much is exposed, an adversary could exploit that knowledge. As with nuclear deterrence, senior decisionmakers will have to balance what to share and what to keep secret.

In contrast, *deterrence by denial* emphasizes the ability to absorb an attack at the time and place it occurs, so rapid, precise attribution of an attack in space may appear relatively less important. However, the line between deterrence by denial and punishment is blurry at best. Strategists might assume that if the threat of denial fails, they still have the threat of punishment to wield. In essence, the threat of punishment usually backstops a denial deterrence strategy. If that is the case, it leads to the notion that both denial and punishment strategies require the same attribution strategy.

An effective attribution strategy will drive the spectrum of technologies, architectures, and decisionmaking processes needed to maintain deterrence. Even with near-perfect technologies for understanding what is happening in space, without a comprehensive attribution strategy for space, many of the attribution challenges outlined above would remain.

The Credibility of U.S. Denial, Space Mission Assurance, and Resilience Efforts

The United States must also ensure that adversaries know U.S. space capabilities can withstand attacks. Weak links make for tempting, first-strike targets and can lead to a breakdown in deterrence no matter where the capabilities physically reside. Increasing satellite and space architectural resilience and defenses can make space a strong link that discourages rather than tempts attack. For the past decade, the Department of Defense has attempted to strengthen deterrence by advancing the concepts of denial, space mission assurance (SMA), and resilience.[4] This approach moves beyond the Cold

War nuclear warfighting context of the deterrence by punishment and denial concepts and focuses on the space domain and today's security dynamics.

Denial, SMA, and resilience approaches for strengthening space deterrence are closely related but there are some distinctions that can be drawn to sharpen these concepts. The goal of denying adversaries the objectives they seek from their space attacks or undesired behavior can be achieved by reducing reliance on space capabilities, developing alternative means of providing these capabilities (perhaps not space-based), or creating resilient space architectures. Alternative concepts of operations (CONOPS) and enhanced training can acceptably reduce Joint Force reliance on space capabilities in some cases. In other cases, such as the positioning, navigation, and timing (PNT) capabilities provided by the Global Positioning System (GPS), there currently is no comprehensive alternative and this places a premium on ensuring delivery of this critical capability or fast-tracking development of an alternative.

Active and passive defense measures such as decoys, escorts, or convoy approaches could be used to strengthen denial capabilities. One interesting historical precedent for covertly strengthening defense capabilities is the "Q Ship" approach, whereby decoys for high-value satellites would be designed to lure adversaries into attacks that could be countered by active defenses. This and other active defense approaches could deter adversaries from attempting attacks. Options include the range of resilience approaches: disaggregation, diversification, deception, protection, proliferation, and distribution. Ongoing commercial programs and plans to deploy very large constellations of low-Earth orbit satellites can be leveraged and should dovetail nicely into the DOD's efforts to enhance resilience.

Credibly communicating the resilience of U.S. space capabilities to a potential attacker and convincing them that it will be unable to achieve its objective is a sticky problem, however. To derive deterrent value from the resiliency of U.S. space capabilities, decisionmakers have to decide the right balance between demonstrating space capabilities' robustness (and/or spotlighting alternative means to accomplish terrestrial military missions), while keeping capabilities' strengths hidden in order to surprise an adversary in conflict, disrupt its plans, and win the fight.

Table 4: Difficulties for Deterrence by Denial in Space

Credibility: Balancing communicating satellite resilience to adversary while maintaining the ability to surprise the adversary if deterrence fails
Credibility: Balance communicating alternatives that enable system resilience without identifying targets for the adversary if deterrence fails
Overemphasis on warfighting could lead to deterrence failure
Overemphasis on deterrence could lead to warfighting failure

As with attribution, decisionmakers must grapple with this tension between the need for transparency and the need for secrecy. Overemphasizing secrecy may allow more warfighting options, but it also might leave a path open for deterrence failure. On the other hand, overemphasizing transparency to signal adversaries might make a war harder to win. Decisionmakers will need to choose their path carefully.

Conclusion

This paper focuses on only a few–but important–areas that would strengthen the overall deterrent value of U.S. space forces and serves as a guide on how to mitigate some weaknesses. It finds that strengthening the deterrent value of U.S. space forces requires a degree of transparency that could weaken the nation's hand should deterrence fail, creating difficult dilemmas for decisionmakers. A thorough assessment of these tensions is in order.

U.S. space strategists need to develop a comprehensive attribution strategy that will cement the adversary perception that the United States has overcome the challenges outlined above. The strategy should define the technologies and decisionmaking processes needed to close this possible path to deterrence failure. It also needs to consider what technical details and other attribution information and data can be appropriately released to the public, or released only to a narrow group of leaders that, in some cases, must include trusted allies and key commercial providers.

To strengthen denial, U.S. strategists should also consider how to best communicate directly or indirectly to potential adversaries the resilience of U.S. capabilities—for example, through public release of information, or demonstrations, or via diplomatic channels. The United States may simply hope its reputation is enough to make credible its ability to attribute attacks or withstand attack—but hope is not a strategy.

References

[1] Defense Intelligence Agency, "Challenges to Security in Space," January 2019 (https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf).

[2] In his foundational analysis on differing perceived attributes of the security dilemma, Robert Jervis calls the situation where actors believe offensive capabilities are dominant and it is difficult to distinguish between offensive and defensive capabilities "doubly dangerous." See "Cooperation Under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (Jan 1978): 167-214.

[3] See for example Thomas Schelling, "Arms and Influence," Yale University Press, New Haven, CT, 1966; and Glenn Snyder "Deterrence and Defense," Princeton University Press, Princeton, NJ, 1961.

[4] Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, "Space Domain Mission Assurance: A Resilience Taxonomy" (Washington: Office of the Secretary of Defense, September 2015).

About the Authors

Dr. Michael P. Gleason is a national security senior project engineer at The Aerospace Corporation's Center for Space Policy and Strategy. Prior to joining Aerospace, he supported the Office of the Secretary of Defense Office of Net Assessment as a senior strategic space analyst. He served 29 years in the Air Force and is an accomplished national security space expert with experience in space policy, strategy, satellite operations, and international affairs. While in the Air Force, he served for five years at the Pentagon and two years at the Department of State. A graduate of the U.S. Air Force Academy, he holds a Ph.D. in international relations from George Washington University.

Peter L. Hays is a retired Air Force Lt Col who works as a defense contractor in the Pentagon supporting the assistant secretary of the Air Force for Space Acquisition and Integration. He has been directly involved in developing and implementing all major national security space policy and strategy initiatives since 2004. Professor Hays currently teaches graduate seminars on "Space and National Security" and "Science, Technology, and National Security Policy" at George Washington University, serves as the space chair at Marine Corps University (MCU), and teaches air- and spacepower seminars at the MCU School of Advanced Warfighting. He previously taught at the Air Force Academy, Air Force School of Advanced Airpower Studies, and National Defense University. Hays holds a Ph.D. from the Fletcher School and was an honor graduate of the Air Force Academy. Major publications include: *Handbook of Space Security*, *Space and Security*, and *Toward a Theory of Spacepower*.

About the Center for Space Policy and Strategy

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The Center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

The views expressed in this publication are solely those of the author(s), and do not necessarily reflect those of The Aerospace Corporation, its management, or its customers.

For more information, go to www.aerospace.org/policy or email policy@aero.org.