SPACE DETERRENCE AND THE GLOBAL POSITIONING SYSTEM: A STRATEGIC IMPERATIVE

AUTHORS:
Christopher M. Stone
Senior Fellow for Space Deterrence

Christophe Bosquillon
Senior Fellow

National Institute FOR Deterrence Studies

THINK DETERRENCE

For more information on this publication, visit
www.thinkdeterrence.com

About the National Institute for Deterrence Studies (NIDS)

NIDS is a 501(C)(3) nonprofit organization that provides national security analysis, policy solutions, and deterrence education. It informs involved or interested parties, while advocating for peace through the responsible application of America's vibrant nuclear deterrent.

NIDS publications do not necessarily reflect the opinions of its donors and sponsors.

Published by the National Institute for Deterrence Studies Fairborn, OH.

Preface

The contributions of the global positioning system (GPS) are unparalleled in the modern world. From second-by-second support to vital communications for the financial, transportation, and other economic sectors, GPS serves as the digital backbone for the bulk of America's warfighting capabilities. American advances in GPS and in the broader positioning, navigation, and timing (PNT) ecosystem spearheaded American leadership in the global space economy. To this day, it remains one of the most successful examples of American space commercialization, leveraging the best of government and private sector activities.

None of this is lost on adversaries, who understand the enormous strategic and operational advantage GPS creates for the United States and its allies. GPS is under continuous attack through such means as spoofing and jamming. Adversary doctrine posits more severe countermeasures, including kinetic attacks, at a much lower threshold than American doctrine considers.

In this thought-provoking paper, Christopher M. Stone and Christophe Bosquillon reiterate the importance of GPS and offer a wide range of options for enhancing space deterrence. They point to the fact that creating GPS resilience—the most often cited American solution—is important for damage limitation but has limited value in deterring adversaries from more severe attacks on the system. Their assessment begins with the need to understand how adversaries think about concepts of space deterrence. From there they assert that the United States needs a much wider range of options.

Stone and Bosquillon offer several specific recommendations and highlight some American initiatives already underway. Space Policy Directive-3, issued in the first Trump administration, identified radio-frequency interference as an important hazard among many to be dealt with through a wide range of measures designed, first, to deepen American understanding of the space environment, and then to apply technical, operational, and policy initiatives to extend and advance the nation's leadership. The authors also point to the need to accelerate GPS modernization efforts, including the L5 signal infrastructure that is key to resilience and mission assurance. While other initiatives are more limited in scope, they still contribute to the fabric of GPS resilience as part of an improved American deterrence strategy. The paper argues for a full spectrum approach to protecting GPS and its vital downstream applications, including threat detection, deterrence, preventative action, and the ability to quickly defeat threats.

Even the tiniest GPS outage would have cataclysmic consequences. Thinking about the future is essential to maintaining a full range of options, even for unthinkable scenarios. The role of GPS in the American economic and security

future requires this kind of thinking and planning to limit the options available to adversaries. Americans are fortunate not to have to think about these things while they use mapping applications and ATMs; rely on the safety of our railway and aviation systems; keep warfighters out of harm's way, and many other applications. It is, however, this thinking that must be done to advance American leadership and protection for the GPS and PNT ecosystem.

Kevin O'Connell, Former Director, Office of Space Commerce

Executive Summary

The global positioning system (GPS) is vital for modern society, providing critical positioning, navigation, and timing (PNT) information essential across numerous sectors, including transportation, finance, and communications. However, as reliance on GPS grows, so does its vulnerability to counterspace attacks from adversaries like China and Russia. These attacks encompass jamming (interrupting satellite signals), spoofing (sending false signals), and more detrimental kinetic attacks that could lead to satellite destruction.

The integrity of GPS is not just a military issue as it also poses risks to civilian lives and essential infrastructure. For instance, incidents of spoofing attacks affecting commercial aviation have surged dramatically, exemplifying the urgent need for GPS protection and complementary terrestrial systems.[1] Attack options vary between reversible methods, like jamming and spoofing, and irreversible actions, including kinetic destruction or electromagnetic pulses (EMP), which can render satellites inoperable.

To effectively deter these threats, the US must understand the strategic culture and perceptions of its adversaries, particularly China, which developed a sophisticated space deterrence strategy that emphasizes both conventional and unconventional capabilities. Chinese military writings indicate a willingness to view perceived infringement of their space rights as justifiable grounds for counterattacks, underscoring the necessity for credible deterrent measures from the United States.

Effective deterrence relies on the ability to impose consequences on adversaries, leveraging robust offensive capabilities and demonstrating resolve. This report positions resilience—defined as a system's capacity to recover from attacks—not as a standalone solution, but as part of a broader damage limitation strategy. Enhancements such as adopting the more secure L5 GPS signal, improved detection mechanisms for jamming and spoofing, and integration of terrestrial navigational systems can mitigate vulnerabilities.

Moreover, we advocate a tiered deterrence framework, targeting various levels of aggression. This involves maintaining a strong defensive posture, active threat engagement, and deploying capabilities that counter adversarial actions prior to escalation. A comprehensive approach to deterrence encompasses not just defense mechanisms against direct attacks but also hedging against multifaceted threats through integrated military and civilian strategies.

In conclusion, the strategic imperative of safeguarding GPS from space-based and terrestrial attacks necessitates a multifaceted approach that includes

learning from adversary behavior, deploying advanced defensive systems, and reinforcing the importance of GPS as critical national infrastructure. Maintaining the integrity of PNT services, now primarily provided by GPS, is essential for national security, economic stability, and everyday societal functions amid rising threats in the space domain.

Space Deterrence and the Global Positioning System: A Strategic Imperative

By
Christopher M. Stone & Christophe Bosquillon

Deterring Space Attack on GPS: A Strategic Imperative

GPS is a vital component of modern life. It provides PNT signals that are essential for a range of applications, from navigation and transportation to energy, finance, and communication. However, the increasing reliance on the largely undefended GPS network, as a key global utility, creates a vulnerability that adversaries are eager to exploit.

Counterspace and terrestrial attacks on GPS satellites and signals, which aim to disrupt or destroy GPS signals and satellite vehicles, are not only a threat but also an attack option currently in use by America's adversaries. Given the criticality of the system and its links to critical infrastructure, both terrestrial and in space, these attacks pose a significant threat to national security, economic stability, and public safety. This report discusses the importance of deterring various types of current and future attacks on GPS and provides guidance on how to achieve this strategic imperative.

Understanding the Threat

Attacks on GPS are launched by a variety of actors and through a multitude of means. Attacks are generally segmented into reversible and irreversible.

Reversible Attack Options

Reversible attack options take several forms. This includes jamming, spoofing, and cyberattacks. Jamming is attributed to radiofrequency (RF) interference, during which adversaries intentionally deny communications between the spacecraft and the ground site or user terminal. GPS signals are vulnerable to jamming since they begin very weak and are even more so by the time they reach the GPS user terminal.

GPS jammers work by interrupting the signals from GPS satellites, making it difficult for a GPS receiver to operate. An oscillator generates an RF signal at the frequency used by GPS devices. This signal is amplified to sufficient strength to overpower or jam GPS signals within a certain range, often with the amplifier's adjustability allowing for flexibility in the jammer's operational scope.

Spoofing is the use of coded counterfeit GPS-like signals, transmitted locally by an adversary. This is done by inducing the receiver to compute incorrect PNT data; the adversary will fool the receiver into thinking it is somewhere it is not. The misleading spoofed signals may be modified to cause the receiver to estimate its position to be somewhere other than where it is and/or at a different time, as determined by the adversary. Spoofing GPS signals, with the aim of not being detected, is a military-grade technology.

A spoofing attack is considerably more complex than a jamming attack, especially if the attack remains undetected. Alternatively, "meaconing" is a type of spoofing where GPS signals are retransmitted, requiring simpler equipment than that required for a spoofing attack. As then-Vice Chief of Space Operations Gen. David Thompson stated, these types of lower threshold attacks happen "every day." The effects of such reversible attacks are not just on military forces but also continue to put the lives of civilians and critical infrastructure at risk. For example, according to *GPS World*, the number of spoofing attacks affecting numerous commercial airlines internationally increased from a few dozen in February 2024 to more than 1,100 in August 2024.[2] Aircraft are not the only target; commercial and military ships are targeted, as well as critical infrastructure.[3]

Irreversible Attack Options

Irreversible attack options on GPS satellites consist of kinetic and electronic destruction, as well as irreversible rendezvous and proximity operations (RPOs). Kinetic destruction is what results from an antisatellite weapon (ASAT), fired terrestrially or in orbit, taking out a specific satellite. Such an attack may create cascading debris, which can destroy all or part of an entire constellation of satellites.

Electronic destruction happens because of an intense EMP that is generated by either the detonation of a nuclear device in orbit or the use of a dedicated EMP weapon precisely targeting a set of satellites or other orbital assets. Irreversible RPOs consist of taking hold of and incapacitating a satellite's ability to function by either mechanical or electromagnetic means or a combination.

All the above apply, not merely to GPS, but also adversary satellite navigation systems. Adversaries are just as

vulnerable in space as the US and its allies. It is for this reason that China established an exceptionally robust terrestrial PNT system with an extensive fiber, clock, and eLoran network. Russia maintains its legacy terrestrial Chayka (Loran-C) network.[4] The consequences of a successful counterspace attack on GPS is severe and may include disrupting navigation and transportation systems, such as aviation and maritime traffic; compromising the accuracy of financial transactions and timing signals; and undermining the effectiveness of military operations and communications systems.

Most contemporary space policy commentators focus on the post-attack effects, namely orbital debris. While it is reported that around 19 percent of all orbital debris impacts medium earth orbit, where GPS operates, most current space debris was not created by kinetic weapons tests or operational uses of such weapons. Rather, debris was generated by the non-passivation of deactivated satellites or spent upper stages traversing in or through such orbital regimes. The main offenders are Russia and China. Depending on the orbital altitude and the number of weapons used, the impacts are less or more damaging. The issue remains, if adversaries' views of deterrence and warfighting in space are different from America's, concerns about second- and third-order effects, while important, are less important than the deterrence of attacks on GPS and the ability for it to survive despite the consequences of a space conflict the US did not start.

The consequences mentioned above are not a future threat but a current reality. There are already daily impacts on American, allied, and commercial assets that are only becoming more threatening to economic and military power. Maintaining American advantage requires a serious analysis of adversary worldviews, deterrence strategies, and warfighting framework to ensure the US has the policy, strategy, and force postures necessary to deter attacks on GPS. If attacks escalate into full-scale war, the system must prove sufficiently capable of limiting the damage to the economy and military forces.

Chinese Space Deterrence

While it is important to understand the types of attack options an adversary can use against American critical space infrastructure targets, it is more important to understand the why behind adversary operations. This allows the US to find a credible means of deterrence against attack. Doing this requires an understanding of the adversary's strategic culture and worldview. Deterrence is primarily accomplished in the mind of an enemy. As China is the primary great power threat and the fastest to develop an adversarial space posture, they are the focus of this paper.

What is Credible Space Deterrence?

Until recently, space warfare, especially kinetic engagements, was often viewed as unthinkable.[5] This view is rooted in the fear of the negative environmental impact of debris generation that would threaten space security. However, the priority of deterrence in national defense policy should be the protection and defense of the nation's critical space infrastructure, not the space environment.

When the United States, or any country for that matter, declares a deterrent threat to an adversary state, in any domain, that threat must be underpinned by a credible resolve to use force, not merely the capability to attribute and absorb attacks.[6] The risk of deterrence failure increases when the threat to respond is not taken seriously. Some commentators argue that rhetoric and threatening statements are dangerous and destabilizing during an already tense situation. [7] However, to be credible, deterrence must be based on more than just words. It relies on armed capability and the perceived willingness to use it.[8]

If a state is willing to retaliate regardless of escalation risk, then most likely the status quo is maintained through deterrence. If, however, a state is perceived as unwilling to follow through on its threats, then the credibility of the threat is degraded, risking deterrence failure. Appearing to do nothing in response to an act of aggression by an enemy demonstrates a lack of will. Standing firm and being willing to assume the costs and risks associated with that threat displays determination. Declaratory policy serves as the mechanism to convey American determination, capability, and political will to deter aggression.[9]

China recognizes the importance of proactivity and decisiveness as a way of bolstering deterrence threats, especially to large constellations like GPS and Starlink. Beijing is exerting its sovereignty and expanding its terrestrial land and sea claims in the South and East China Seas by establishing economic exclusion zones, air defense identification zones, building islands with military bases, and reinforcing its coastal eLoran system—ensuring terrestrial PNT service up to 1,000 nautical miles offshore (far beyond Taiwan). There are concerns that the rapid deployment of Chinese counterspace capabilities and its aggressive behavior in the Pacific, on orbit, could lead Beijing to assert it has the legal right to attack foreign spacecraft overflying Chinese territory. [10] This would have serious repercussions on current customary norms such as freedom of overflight that have existed since Sputnik 1.

China's Unique Views on Space Deterrence

The Chinese People's Liberation Army (PLA) space forces and their political leadership in the Chinese Communist Party (CCP) have a well-developed space deterrence concept undergirding general deterrence, which is supported by a growing space weapons capability. As one Chinese document highlights, "…when another state conscientiously infringes upon China's space rights and interests and causes harm to national space security, China [may] implement space deterrence against the enemy and launch a space counterattack."[11]

In the PLA's writings on space warfare and deterrence, the development of "real capabilities" for space attack is considered an "integral part of battle planning by the People's Liberation Army in any future conflict."[12] This not only includes states of war, but also "periods of tension."[13] Space forces, unlike nuclear forces, are considered by Chinese military leaders to be subject to a much lower threshold of use, and therefore "space strategic power must not only have a deterrent effect, but real warfighting potential."[14]

In the Chinese language, the definition of deterrence is different than that of the West. While the United States views deterrence as the prevention of war through cost/benefit calculation and attempts at controlling perceptions, the Chinese term *weishe* is a combination of coercive, proactive force and self-defense.[15] The focus of space deterrence operations is to deter behavior that endangers China's interests by enhancing deployed military capabilities.[16] To do this requires "powerful comprehensive national power" in space and terrestrially, that supports the overarching general or "integrated-whole" deterrence strategy.[17]

While space support capabilities are very important to the PLA space strategy, they alone are not what creates a deterrent effect. For the Chinese, having a credible "attack to deter" capability in space to threaten other nations' space capabilities is where their deterrence of the adversary's space capabilities resides. "In this way, both sides are reluctant to attack the other's space assets lest they also come under attack."[18]

In addition to having credible space attack weapons for effective deterrence and warfighting, the Chinese advocate that they should reveal "firm resolve to dare…and use this capability" to create "certain psychological pressure on and fear in the adversary, and [force] the adversary to dare not to conduct space operations with initiative." PLA strategists argue for conducting "limited space operational activities" that include "warning and punishment as goals."[19] The overarching objective of space deterrence is to "choose appropriate deterrence means to display the horribleness, severity, and

urgency of the consequences."[20] This type of space deterrence, which might be called "space deterrence with Chinese characteristics", suggests how China views space warfighting. The Chinese write about how the United States will have to deal with the "grave aftermath" and the impact that "rapid and destructive" space warfare will have upon its space-enabled society and armed forces.[21]

It is important to note that, while China has a formidable and growing offensive space deterrent force, China currently has a lower dependence on space-based capabilities than the US. This is due to several factors. First, China invested heavily in advanced ground-based technologies, such as terrestrial communication, surveillance, timing, and navigation systems, which can fulfill many functions traditionally served by satellites. Second, China utilizes high-altitude balloons and uncrewed aerial vehicles for reconnaissance and communication, reducing a total reliance on satellites for similar tasks. Third, China's military strategy focuses on multiple layers of redundancy. This means that if one system fails or is targeted, others can take over, thus minimizing the overall reliance on any satellite constellation for its mission utilities. Fourth, advances in technologies, such as radar and electronic warfare systems, allow for effective ground and air operations without needing extensive satellite support. Fifth, by combining military and civilian space initiatives, China can leverage its resources more effectively, allowing for flexible strategies that do not overly rely on space systems for national security. Sixth, China's goals for self-sufficiency and independent development in technology—leveraging intellectual theft of Western intellectual property—enables the country to build and maintain capabilities within its borders without relying too heavily on external satellite communications and resources. While this is a longstanding approach, President Xi Jinping directed that space be fully integrated into economic and military operations for the regime, and this reliance becomes more of a risk for US and allied exploration in the future.

Deterring Space Attacks on GPS

As noted above, China has an active attack-to-deter approach to space deterrence. The American framework for assessing and developing a credible deterrence posture must be based on a realistic assessment of what an adversary believes, avoiding mirror-imaging. This requires innovative thinking and the development of a tailored framework for implementing reliable space deterrence. Such a framework requires acknowledging three key items.

First, strategists and policymakers must acknowledge that space is an offensive dominant domain. As a result, effective deterrence in space requires the United States actively protect its

space systems through a credible counterforce capability.

Second, any future national security space posture should acknowledge that damage limitation measures, such as the active defense of critical American space and terrestrial infrastructures, are vital to ensure credible deterrence. Deployment of active defenses supports the view expressed by deterrence scholars, such as Keith B. Payne, who argue that exercising force projection requires management of risk to the homeland and deployed forces. This includes damage limitation measures such as "offensive capabilities for counterforce strikes; active defenses such as air and ballistic missile defenses; and passive defenses such as physical protection;" and hardening against space-borne electromagnetic pulse attacks.[22]

Third, policymakers and strategists must view space systems as a critical infrastructure of the United States and not just a support structure for force enhancement and terrestrial operations. Though this concept is evident in national strategy and doctrine, it lacks a commensurate level of funding or support from senior leadership.

Resilience and Complementary PNT

According to current Department of Defense (DoD) policy, resilience refers to "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, despite hostile action or adverse conditions."[23] While the term "resilience" is rightly seen as an important design feature, it has come to mean everything from a defense tactic to deterrence itself, which is a fallacy. It is important to realize that resilience is not a deterrent or a defense. Rather, resilience is only one part of what is known as damage limitation. In other words, "deterrence by denial," if it was ever a valid concept, is not applicable in the GPS context.

Resilience is the ability to face an attack and continue operating, or more specifically, the "ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability."[24] While this term is central to the current DoD view of deterrence as well as defense, it is interesting to note how the taxonomy acknowledges its lack of effectiveness in implementation.

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.[25]

In other words, it is hard to know how resilient a specific constellation is within its own system design or how to make an already deployed constellation more resilient due to updates in adversary space weaponry. As such, resiliency alone will not deter attacks as shown in real-time by both Chinese and Russian attacks on GPS signals and systems worldwide. However, since a robust set of complementary, terrestrial PNT capabilities are not deployed in most of the West, it remains to be seen what type of impact, in addition to damage limitation, these systems could have in support of deterrence in the adversary strategist's mind.

Space Force GPS Damage Limitation Options

First, track GPS jamming and spoofing in real-time and provide improved situational awareness to the chain of command. In mid-January 2025, the Space Force awarded Slingshot Aerospace a $1.9 million small business innovative research phase two contract.[26] The intent is to refine its GPS interference detection technology. The contract originated with Space Force's SpaceWERX innovation unit following a $1.9 million phase one contract awarded in 2021, which tasked Slingshot with developing an initial capability through its data exploitation and enhanced processing system. This contract, positioning, navigation, and timing-secure electronic navigation threat intelligence and location (PNT-SENTINEL), aims to improve the system's modeling capabilities by incorporating advanced artificial intelligence, machine learning, and predictive analytics. The PNT-SENTINEL system, if fully fielded, will take advantage of a mesh network of thousands of satellites to identify locations on the ground where GPS signals are jammed or spoofed.

Second, accelerate the implementation of L5 signal infrastructure. At present, the L5 signal is part of the GPS modernization plan and is gradually implemented as the constellation is renewed. However, as a new capability, L5 faces several obstacles delaying its adoption. First, the GPS L5 signal is broadcast by 17 of 31 GPS satellites, whereas L5 operational capability requires 24 satellites broadcasting it, something not expected until 2027. Second, the L5 signal is considered "preoperational" and not yet fully certified for critical applications. Most GPS receivers are not equipped to use L5 signals, which stalls adoption. Third, the implementation of the GPS next-generation operational control system, known as OCX, which is crucial for fully leveraging L5 capabilities, is years behind schedule. These factors collectively contribute to the slow adoption of the L5 signal.

L5's advantages, in terms of accuracy and interference resistance, are fully leveraged once L5 is used autonomously, rather than combined with L1. Despite the availability of L5 signals for a decade, most devices still depend on outdated L1 signals and have not fully integrated L5. Dual-frequency devices are constrained by the need to first acquire L1 signals before accessing L5, limiting their effectiveness in jamming scenarios. Many military allies, contractors, and civilian infrastructure operators rely on vulnerable L1 signals, lacking access to more secure military GPS signals.

Another option for the L5 signal is oneNav's developed L5-direct.[27] This capability enables devices to directly acquire L5 signals without needing L1, significantly enhancing GPS resilience to jamming.[28] Field studies conducted in 2024, particularly near the Polish/Russian border, confirm the superior resilience of L5 signals to jamming attacks. Adoption of L5-direct technology could protect essential military and civilian technologies from interference, providing better security and reliability. This could serve as a blueprint for enhancing GPS resilience in conflict zones and critical industries like aviation.

Overall, governments could consider investing in upgrading GPS infrastructure and mandating the use of L5 signals in critical GPS-enabled technologies. Critical infrastructure sectors should evaluate and adopt L5-direct technology to mitigate the risks of GPS jamming. Military alliances and civilian agencies should collaborate to ensure a unified approach to adopting L5-direct technology, ensuring compatibility and broader protection. Airlines and aviation authorities should incorporate L5-direct solutions to ensure navigational safety and reliability amid increasing GPS interference. Continued research and development are essential to improve L5 signal technology and address emerging threats, maintaining a technological edge over adversaries. Continued investment in and development of L5-compatible devices and processors will be essential for widespread adoption and enhanced security against GPS jamming. Implementing these changes will significantly enhance the security and reliability of GPS-dependent systems, reducing the risk of interference.

Other Ground-based GPS Supplements

There exist other ground-based solutions that are less susceptible to jamming and spoofing than GPS. However, it is important to understand that such solutions are merely supplements for damage limitation; they do not constitute alternatives to GPS nor are they a component of a robust deterrence architecture.

Enhanced long-range navigation (eLoran) is a modernized version of the Loran-C system, providing accurate positioning and timing. [29] The advantages of the system include its resilience to jamming and spoofing and wide-area coverage. Its cons are its limited accuracy compared to GPS and the large transmitters required.

Cellular networks are also an option because 4G/5G networks offer an option for navigation and timing. The advantages of using cellular networks are their ubiquity in urban areas and the fact that they support device authentication. The disadvantages are their ineffectiveness in remote areas and their susceptibility to local outages.

Wi-Fi positioning systems utilize Wi-Fi access points for navigation in indoor/urban environments. The advantages of the systems are their high precision in covered zones and their complementarity with GPS indoors. Their disadvantage is their limited range and scalability.

Ground-based beacons and navigation aids like very-high-frequency omnidirectional, distance measuring equipment, and instrument landing systems for aviation. These systems are well-established and reliable. They are, however, limited to specific sectors like aviation and have low versatility.

Implementing Deterrence and Damage Limitation Measures

Implementing deterrence measures against space attacks on GPS is required. Policymakers have many technological options to improve deterrence and damage limitation, both of which protect GPS satellites, signals, and users. This requires thoughtful and deliberate consideration of costs, effectiveness, implementation schemes, and timelines to arrive at a solution set that best serves the nation. As such, efforts to deter attacks and provide damage limitation require sustained effort and commitment from government, industry, and civil society. Some key steps include developing and deploying GPS and complementary resilient PNT systems. They should include systems using multiple frequencies as well as terrestrial and allied-based PNT capabilities. Federal policies, including those within the DoD, highlight the importance of the space sector to the many other parts of defense and national critical infrastructure. Recent reports highlight the fact that growing interdependencies between critical infrastructure areas, such as communications, transportation, energy, and defense, create a potentially large cost in human life and/or economic markets if they fail.

Criteria that define what make infrastructure within the United States critical include four key factors. First, it

provides routine functions along operational paths essential for average or routine system function. Second, no rapid substitutes exist. Third, sudden dysfunction in and around these elements causes nontrivial harm. Fourth, they are embedded in wide, functionally reciprocal, and integrated systems. The more critical that these interdependencies become, the larger the cost of failure.

One small part of the larger space sector that is interdependent with the transportation, defense, energy, and other infrastructure sectors is reliance on the GPS navigation and timing signals. As one report states, "Because of the increasing reliance of transportation upon GPS, the consequences of loss of the GPS signal can be severe (depending upon its application), in terms of safety and…economic damage to the nation."[30] Another vulnerability related to GPS is the reliance of energy infrastructure on GPS timing signals.

One report summarizes this concern saying, "GPS has emerged as a key component of the power generation and distribution network monitoring systems for data collection, fault detection, vulnerability mitigation, and recovery. With its continued market penetration, the value of GPS to the power industry is likely to grow, along with the impacts of unanticipated disruptions."[31] Achieving resilience for damage limitation from current and future GPS attacks must be treated seriously and requires the funding and the weapons systems capable of deterring and, if necessary, defeating such attacks.

Just as PLA space systems are tied to the homeland defense of the Chinese mainland, space systems are also a part of the American homeland defense infrastructure. Therefore, any future American space deterrence concept must be tied into the homeland defense strategy of the United States. This fits with the present definition of homeland defense, which is "the protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression."[32]

The DoD states in its previous doctrine that the United States executes homeland defense "by detecting, deterring, preventing and defeating threats from actors of concern as far forward from the homeland as possible."[33] In national strategies of the past, space was acknowledged as vital, requiring coordination between services and agencies to ensure that external threats do not impede societal operations and the continued protection of life and property.

Accomplishing this requires the following actions. First, the US must detect threats in the forward region of space, which requires space situational awareness (SSA). While there are tremendous efforts to improve SSA,

more must be done to achieve the level of situational awareness needed.

Second, the US needs a concerted effort to achieve deterrence in space. The terms deterrence and defense are used in policy and strategy in DoD. In practice, however, there is no real deterrence capability specified or funded in the Space Force's budget. This must change.

Third, preventive action is required. This takes the Chinese concept of "attack to deter" and applies it to homeland defense of critical space infrastructure, such as GPS. If a threat materializes, such as the 400 percent increase in GPS spoofing and jamming attacks, the US must take action to prevent attacks in the future.

Fourth, the United States must have the ability to defeat threats to the homeland. This requires capabilities and the political will to engage and defeat threats as far from the homeland as possible. Engaging and defeating threats to GPS in and from space is much more effective than waiting for an attack, whether cyber or conventional.

Rapidly Deploy a Tiered Deterrence Force Structure

China's counter-intervention strategy in the Pacific combined with its strategic culture, warfighting doctrines, and space force developments and deployments, require American strategists create a national security space strategy that supports and acknowledges the importance of homeland defense and the core interests of the United States in the Pacific. To do this requires shaping capabilities and support infrastructure into an operational framework capable of providing the president with the capabilities needed to address each of the potential types of deterrence scenarios required. Adapting Herman Kahn's tiered approach to deterrence requires the United States to build a three-tier framework.[34]

Tier I deterrence addresses the Chinese view of a nuclear-spacepower nexus that they term "strategic deterrence." The survival of the CCP and the PLA in the context of their space-enabled counter-intervention strategy creates an escalation dominance effect should the United States not create a capability that drives friction in Chinese planning. This requires publicly declaring that the United States will not tolerate interference or attacks on systems that support nuclear command and control. Such activity is considered escalatory and threatens stability between the two nations and the survival of the US homeland, supporting critical infrastructure and the American people. This requires the posturing of American space forces forward from sea and air launch sites, as well as posturing nuclear forces as a strategic communication to Beijing.[35]

Tier II deterrence addresses the build-up of Chinese terrestrial and orbital counterspace forces to threaten American space infrastructure's ground and space segments. This deterrence requires a multilayered counterspace portfolio capable of providing the president with multiple options. These include preventative attacks on adversary ASAT garrisons, directed energy weapons, and space-based intelligence, surveillance, and reconnaissance (ISR) assets. The goal of these strikes is to achieve a limited war aim of self-defense of American space systems. In addition, it can also support a larger aim, such as the creation of friction, uncertainty, and disunity in Chinese command and control.[36]

Tier II deterrence requires the development and deployment of a survivable nuclear triad of capabilities utilizing a joint or allied combined force concept on land, air, and sea. On land and sea, the US can deploy a modified version of the Aegis-Standard Missile-3 in a ring around the Western Pacific from Alaska down through Australia and India. Coupled with sensors already in theater and with those in geosynchronous orbit for SSA, these weapons have the ability to not only achieve a low or medium earth orbit ASAT capability against potential adversary ISR assets but can provide a notional space reconstitution denial system at mid-course altitudes. Finally, these systems can provide a means to defend American assets against terrestrially launched ASAT missiles fired from deployed "mobile warfare" locations.

Finally, the sea- and land-based legs of the counterspace triad include air-launched ASAT capabilities that can be based overseas or at home as part of a new global space sovereignty alert force, capable of engaging targets in all orbital planes and at varying altitudes. The technology for this is also available through several research and development programs going back decades. This includes the successfully tested Celestial Eagle concept and the Defense Advanced Research Projects Agency's former Airborne Launch Assist Space Access (ALASA) program. ALASA provided a low-cost means to launch satellites into orbit and can serve as an ASAT platform as well as an operationally responsive, low-cost reconstitution method for some mission areas and orbital altitudes. The ability to relocate and launch quickly from virtually any major runway around the world substantially reduces the time needed to launch a mission. Launching from an aircraft provides launch-point offset, which permits any orbit direction without concerns for launch direction limits imposed by geography at fixed base launch facilities.

Tier III deterrence requires only reversible counteraction. It leverages the purposeful interference norm of behavior as deterrence or retribution to terrestrial actions or actions against

space segment assets. This requires a series of capabilities to negate signals or types of signals in an entire channel, sets of channels, an entire transponder, sets of transponders, a satellite, a constellation of satellites, all satellites flagged by the adversary, or all satellites that are suspected of aiding the adversary in counter-intervention efforts. This provides a debris-free alternative, provided that the adversary does not see the benefits of escalation to kinetic exchanges. This creates a potential for deterrence through the threat of a "soft kill" against adversary capabilities—creating lower levels of escalation dominance.[37]

Each of these tiers requires a tailored approach, given the different potential adversaries. In the case of China, a more aggressive approach, based on escalation dominance, inverts the Chinese decision cycle in favor of the United States and its allies. A decision tool is required for strategists and commanders to enable them to rapidly decide what course of action adversary patterns are highlighting, how to stay ahead of their decisions, and how to effectively confuse and paralyze the adversary. One method is through the creation of a space warfare escalation ladder (Table 1).

As with Herman Kahn's escalation ladder for nuclear warfare, a space escalation ladder is intended to serve as a tool for decision-makers to assess the situation and stay ahead of an adversary's decision cycle by observing the patterns of strategic and operational behavior and re-orienting American space and terrestrial forces to rapidly escalate into a position that prevents the destruction of critical space systems. Such a ladder is not all-encompassing and provides only a few examples of adversary actions within each threshold to provide context.

It is important to note that just because this table shows a step-by-step method of escalating space engagements from peacetime to total war, an adversary is not limited to starting with reversible means and staying there or gradually escalating. Indeed, as the Chinese way of offensive space deterrence highlights, depending on the decision calculus and the perceived level of opportunity or danger in a given situation, PLA space forces can very well conduct an offensive combining several thresholds or go directly to a destructive attack.

The first threshold, which is based on noninterference or peaceful use of space, is the ideal peacetime condition that current DoD space policy promotes. This describes conditions intended by international space legal regimes, such as freedom of action in space for civil space exploration, commercial space development, and military uses of space for national and multinational interests. It also includes military operations such as intelligence and space situational awareness to ensure the status quo is maintained by all spacefaring nations.

Once a state, such as China, crosses the threshold of reversible, yet purposeful, interference, the escalatory requirements for observing interference, the escalatory requirements for observing the jamming, laser tracking, or dazzling type behavior requires a sufficient response from American leadership to achieve a higher level of escalation through a combination of offensive and defensive capabilities as well as adversary uncertainty.

Once a state, such as China, crosses the threshold of reversible, yet purposeful, interference, the escalatory requirements for observing interference, the escalatory requirements for observing the jamming, laser tracking, or dazzling type behavior requires a sufficient response from American leadership to achieve a higher level of escalation through a combination of offensive and defensive capabilities as well as adversary uncertainty.

Table 1. Space Deterrence Escalation Ladder. Stone, Reversing the Tao, 2015.

Non-interference/Peaceful Use of Space
1. Freedom of action in space (civil, commercial, military use, benefit of nation and world)
2. Intelligence/Space Situational Awareness Collection (Passive/Active)
Reversible, Yet Purposeful Interference Threshold (Deny/Degrade)
1. Passive jamming
2. Active jamming/cyber attacks
3. Laser tracking/dazzling
4. Unauthorized, rendezvous and proximity operations (RPO) near U.S./allied spacecraft
5. Posturing/mobilization of destructive space attack forces
Irreversible, purposeful interference threshold (Damage)
1. High energy chemical laser attack
2. High power microwave weapons use
Kinetic, debris generation threshold (Destroy)
1. Kinety energy (KE) anti-satellite (ASAT) missiles (terrestrial based-LEO)
2. Kinetic energy (KE) anti-satellite (ASAT missiles (co-orbital)
3. Kinetic energy (KE) anti-satellite (AST) missiles (terrestrial based-GEO)
Nuclear use threshold (Destroy)
1. Terrestrial Fractional Orbital Bombardment Systems (FOBS)
2. Orbital electro-magnetic pulse (EMP)
3. Orbital nuclear strike against spacecraft (all orbital regimes effected)

Once an adversary progresses up the space escalation ladder, American leaders can choose to allow the adversary to continue denying and degrading American systems or escalate to a higher level to encourage cessation of the interference or attack. Once the kinetic threshold is crossed, the destruction of American space assets is the adversary's clear objective within their destructive space warfare concept. This could be terrestrial-based ASAT attacks or space-based co-orbital ASATs. Directed energy weapons, such as high-power microwaves or lasers, are also a possibility. As the situation escalates, the maximum possible damage is a more extreme scenario where the adversary decides to destroy all threats to its national survival by detonating nuclear weapons in space to deny the benefits of space and create severe havoc to the space continuity of the government of the United States.

Conclusion

Deterring attacks on GPS critical space infrastructure is a strategic imperative that requires a comprehensive approach. This requires an understanding of the adversary's strategic culture and force structure. It also requires building a space deterrent force and damage limitation capabilities. These must consist of complementary terrestrial PNT systems capable of deterring adversary attacks of all types while defeating any attack.

By incorporating these measures into a robust and credible space deterrence posture, the United States can reduce the risk of adversary attacks on GPS and ensure the continued reliability and accuracy of GPS signals. Given societal dependence on GPS, the nation must prioritize the security and resiliency of this critical infrastructure. Such a process requires more focused and dedicated leadership to ensure America's PNT needs are met.

Endnotes

[1] Editor, "Near Loss of Aircraft, Major Disruptions at Denver and Dallas—One Page Grabbers." *RNTF*, March 28, 2023, https://rntfnd.org/2023/03/28/near-loss-of-aircraft-major-disruptions-at-denver-and-dallas-one-page-grabbers.

[2] Jesse Khalil, "GNSS Spoofing Threatens Airline Safety, Alarming Pilots and Aviation Officials," *GPS World*, September 24, 2024, https://www.gpsworld.com/gnss-spoofing-threatens-airline-safety-alarming-pilots-and-aviation-officials.

[3] Jesse Khalil, "Alleged North Korea GPS Jamming Disrupts Flights and Ships in South Korea," *GPS World,* November 12, 2024, https://www.gpsworld.com/alleged-north-korea-gps-jamming-disrupts-flights-and-ships-in-south-korea-for-second-day.

[4] Jesse Khalil, "China Completes National eLoran Network," *GPS World*, October 7, 2024, https://www.gpsworld.com/china-completes-national-eloran-network.

[5] Michael Krepon, *Anti-Satellite Weapons, Deterrence and Sino-American Relations*, Stimson Center, September 2013, https://www.stimson.org/wp-content/files/file-attachments/Anti-satellite%20Weapons%20-The%20Stimson%20Center.pdf

[6] Herman Kahn, *On Thermonuclear War* (Princeton University Press, 1960), 146-47.

[7] Scott Sagan, "The Korean Missile Crisis," *Foreign Affairs* (November/December 2017), 76.

[8] James Payne, *National Security and Foreign Policy* (Lytton Publishing, 1981), 54.

[9] William J. Perry and James R. Schlesinger, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: US Institute of Peace Press, 2009), 35. https://www.usip.org/strategic-posture-commission/view-the-report.

[10] US-China Economic and Security Review Commission, *China's View of Sovereignty and Methods of Access Control,* 110th Congress, 2008, statement of Philip Meek. It is worthwhile to note the actions of the Kingdom of Tonga to claim key slots in the geostationary orbital belt, prime space real estate for space-based communications. See Edmund L. Andrews, "Tiny Tonga Seeks Satellite Empire in Space," *The New York Times*, August 28, 1990, http://www.nytimes.com/1990/08/28/business/tiny-tonga-seeks-satellite-empire-inspace.html?pagewanted=all.

[11] Sun Zhaoli, *Science of Strategy* (Military Science Press, 2013), 238.

[12] Ibid., 238.

[13] Ibid., 239.

[14] Ibid., 239.

[15] Dean Cheng, "Chinese Views on Deterrence." *Joint Force Quarterly* 60 (2011), 92, https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-60.pdf.

[16] Zhaoli, Science of Strategy, 238.

[17] Zhaoli. Science of Strategy, 194.

[18] Kevin Pollpeter, "The Chinese Vision of Space Military Operations," in *The Paradox of Power* (NDU Press, 2011), 342.

[19] Zhaoli, *Science of Strategy*, 234.

[20] Zhaoli, *Science of Strategy*, 192.

[21] Joan Johnson-Freese, *Space as a Strategic Asset* (Columbia University Press, 2007), 222.
[22] Keith B. Payne, "The Great Divide in US Deterrence Thought," *Strategic Studies Quarterly* 14, 2 (2020), 16, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-2/SSQSummer2020.pdf?ver=2020-05-27-132858-983.

[23] Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, "Space Domain
Mission Assurance: A Resilience Taxonomy," (Assistant Secretary of Defense for Homeland Defense & Global Security, September 2015), https://policy.defense.gov/Portals/11/Space%20Policy/ResilienceTaxonomyWhitePaperFinal.pdf?ver=2016-12-27-131828-623

[24] Ibid., 3.

[25] Ibid., 3.

[26] Sandra Erwin, "Slingshot Tracks Electronic Interference Targeting GPS Signals," *Space News*, January 15, 2025, https://spacenews.com/slingshot-tracks-electronic-interference-targeting-gps-signals.

[27] "Home Page," oneNav.ai, April 30, 2025, https://onenav.ai.

[28] Sandra Erwin, "GPS Startup Bets on Advanced Signal to Counter Jamming Threats," *Space News*, July 17, 2024, https://spacenews.com/gps-startup-bets-on-advanced-signal-to-counter-jamming-threats.

[29] "Enhanced Long-range Navigation-eLORAN," Stanford Engineering GPS Lab, April 30, 2025, https://gps.stanford.edu/research/early-gpspnt-research/enhanced-long-range-navigation-eloran.

[30] US Department of Transportation, *Vulnerability of the Transportation System Reliance on the Global Positioning System* (The National Transportation Systems Center, August 2001), ES-6.

[31] US Department of Transportation, *Global Positioning System Timing Signal Criticality Update,* (The National Transportation Systems Center, July 2008), xii.

[32] Department of Defense, *Joint Publication 1-02: Dictionary of Military Terms* (2015), https://irp.fas.org/doddir/dod/jp1_02.pdf.

[33] Department of Defense, *Joint Publication Joint Publication 3-27: Homeland Defense* (2015), https://irp.fas.org/doddir/dod/jp3_27.pdf.

[34] Christopher Stone, "Reversing the Tao: A Framework for Credible Space Deterrence" (master's thesis, Missouri State University), https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=2506&context=theses.

[35] Ibid.

[36] Ibid.

[37] Ibid.

About the Authors

Christopher Stone is Senior Fellow for Space Deterrence at the National Institute for Deterrence Studies. He is a former Special Assistant to the Deputy Assistant Secretary of Defense for Space Policy, U.S. Senate staffer, and U.S. Air Force space operations officer with more than twenty years in space operations, policy and strategy. In addition to his role as senior fellow, Stone serves as Associate Editor for Space Deterrence and Conflict for Global Security Review and is the host of the Real Space Strategy podcast.

Christophe Bosquillon is a Senior Fellow at the National Institute for Deterrence Studies. Building up on geopolitical and strategic insights acquired as a multi-decades Indo-Pacific resident, he focuses on adversarial threats implications for space defense, economy, and policy.

The views expressed are the authors' own and do not necessarily represent the views of the National Institute for Deterrence Studies, its staff, donors, or sponsors.

Acknowledgements

The authors would like to thank Kevin O'Connell, former Director of the Office of Space Commerce U.S. Department of Commerce, for agreeing to review the paper and provide the preface. His thoughtful comments made our paper a more effective result.

Limited Print and Electronic Distribution Rights

Gifts from NIDS supporters and income from operations provided funding for this NIDS document.