Extended Space Deterrence: Providing Security Assurance in Space

Kiseok Michael Kang
Georgetown University, kk1325@georgetown.edu

Follow this and additional works at: https://digitalcommons.usf.edu/jss
pp. 11-25

Recommended Citation
Available at: https://digitalcommons.usf.edu/jss/vol16/iss2/2

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.
Extended Space Deterrence: Providing Security Assurance in Space

Abstract
Many U.S. allies are increasingly dependent on space-based platforms for their military and economic activities. At the same time, the counterspace threats from U.S. adversaries such as China and Russia are rapidly intensifying. The United States has provided extended deterrence to its allies through its overwhelming nuclear and conventional capabilities for decades. The question arises as to whether the time-tested logic of extended deterrence is applicable in the space domain. This research argues that U.S. extended deterrence in space—relying on the traditional mechanism of deterrence-by-punishment—is ineffective due to the unique nature of outer space.
Introduction

The U.S. allies’ ever-increasing activities in space for military and economic purposes create both opportunities and risks for Washington. It presents opportunities as the allies’ space-based assets can provide support to coalition operations. For instance, the United Kingdom’s military communications satellites (SATCOM) known as Skynet contributed to the North Atlantic Treaty Organization (NATO) operations in Afghanistan. The Japanese positioning, navigation, and timing (PNT) service known as Quasi-Zenith Satellite Systems (QZSS) can augment the U.S.-operated Global Positioning System (GPS) in the Indo-Pacific region. However, these space assets are also vulnerable to adversaries’ malicious activities. The counter space capabilities of U.S. adversaries such as China, Russia, North Korea, and Iran are growing at a rapid pace. Subsequently, the allies expect the United States—the far-dominant space power—to play a role in deterring the adversaries in space. In other words, allies anticipate Washington’s commitment to extended space deterrence.

Extended deterrence—seeking to prevent an adversary’s harmful action against a third party—has been a main foreign policy tool of the United States for decades. Providing the nuclear umbrella and tripwire forces to its allies, the United States could keep enemies at bay and maintain the “long peace” during the Cold War. During this period, the crux of the United States extended deterrence strategy was that the United States would respond forcefully against any act of aggression, conventional or nuclear, against its allies. Nonetheless, in the age of expanding warfighting domains where emerging technologies enable states to advance their geopolitical interests without triggering a full-scale conflict, it is uncertain whether the theory of deterrence is still pertinent. In the aftermath of the 9/11 terrorist attacks which cast doubt on the utility of deterrence against asymmetric threats, the New York Times editorial argued that “the logic of deterrence transcends any particular era or enemy.” In this context, the aim of this article is to provide an answer to the research question of whether the theory of extended deterrence can transcend traditional domains and be extended to the space domain.
Deterrence in Space

Deterrence

Deterrence can be broadly defined as “the power to dissuade” others from taking an action by convincing them that the prospective costs of the action outweigh its prospective gains. It is one of the most widely and persistently studied subjects in the field of international relations (IR). Robert Jervis posits that it is “the most influential school of thought” in the American IR scholarship. Deterrence also has been a core pillar of the U.S. grand strategy since World War II and especially played a significant role during the Cold War. The early works on deterrence focused on nuclear deterrence that employs the threat of nuclear reprisal to dissuade. After the end of the Cold War, scholars challenged the relevance of nuclear or large-scale conventional deterrence and instead attempted to address deterrence against asymmetric threats. This article fits into this new wave of deterrence research as it seeks to study how the longstanding logic of deterrence can be applicable in the space domain.

Scholars and practitioners distinguish between different mechanisms of deterrence. Deterrence by the punishment threatens to inflict intolerable damage through retaliation, thus manipulating an adversary’s perception of costs. The Eisenhower Administration’s policy of massive retaliation is a classic example of such an approach. On the other hand, deterrence by denial seeks to build formidable defense capabilities that can deny or reduce an adversary’s benefits from aggression. Some argue that a deterrence-by-denial strategy can be more effective against asymmetric threats such as terrorist or cyber-attacks. Others argue that policy-makers should pursue non-military approaches such as deterrence by entanglement and by norms to deter gray zone threats. This article contributes to the policy debate by discussing the usefulness of different deterrence mechanisms in the space domain.

The deterrence literature underscores two factors that determine the efficacy of dissuasion mechanism: A defender’s capability and the credibility of its threat. First, a defender should possess enough capability to punish the potential aggressor. In nuclear deterrence, this means whether a country can launch powerful nuclear retaliation. In conventional deterrence, theorists focus on the balance of military capabilities. Second, credibility is an essential component of effective
deterrence. As Thomas C. Schelling famously puts it, deterrence is not about estimating enemy capabilities but influencing their intentions. The hardest part of deterrence, according to him, is communicating one’s intentions. Credibility is also key in establishing successful extended deterrence.

Extended Deterrence

It is important to note the difference between direct and extended deterrence. Direct deterrence is about discouraging attacks on a country’s homeland while extended deterrence seeks to prevent attacks on a third party, such as an ally. Scholars agree that credible extended deterrence is more challenging since a party that bears the costs of deterrence differs from a beneficiary of deterrence. Thus it requires additional efforts to convince a potential aggressor that the provider of extended deterrence will retaliate on behalf of its protégé.

Extended deterrence holds no less significance than direct deterrence for the United States and other great powers that need to manage their vast networks of allies. The famous question of how to convince the Soviets that the U.S. government was willing to risk New York for Paris highlights the nature of the challenge. The failure of extended deterrence arguably led to both world wars. To resolve this inherent credibility problem in extended deterrence, Schelling and scholars suggested a tripwire, a small token force deployed to the protégé’s territory by the provider of extended deterrence. During the Cold War, for example, Washington forwardly deployed its forces around the world which contributed to the stability of some regions.

Space Extended Deterrence

Before discussing the difficulties of extended space deterrence, I should clearly define what space deterrence is and is not. Scholars define space deterrence as preventing an adversary’s hostile actions against both space-based assets and terrestrial systems that support space operations by “whatever means.” Unlike nuclear deterrence, the focus is on “the nature of the target, not the nature of the weapon.” Likewise, space-extended deterrence can be defined as dissuading an adversary from harming a third party’s space assets.

Building credibility for space deterrence is particularly challenging due to the problems of proportionality and attribution. First, it is hard to
establish a credible threat of retaliation—that is both proportional and consequential—against attacks on space assets. Responding in kind, threatening to target an adversary’s space assets, is proportional, but hardly consequential since U.S. adversaries are less dependent on space assets. Scholars have suggested cross-domain retaliation to impose costs as a solution to deter asymmetrical threats such as cyberattacks. However, as James Lewis argues, launching massive retaliation against the loss of a satellite is “ridiculously disproportional” and the threat will not be credible. Second, scholars argue that attribution, which is a critical part of successful retribution, is difficult in space because of the great distance between the space assets and ground components, a multitude of space actors, and the possibility of natural phenomena such as geomagnetic storms.

The problem of credibility further exacerbates as a state attempts to extend deterrence to prevent harm against its allies’ space assets. The ambiguity in attribution and challenges of proportional response can impede the provider of extended deterrence’s willingness and ability to retaliate forcefully on behalf of its client. There is a notable gap in the emerging space deterrence literature on the dynamics of space-extended deterrence. The aim of this research, therefore, is to investigate the challenges the United States confronts in providing space-extended deterrence to its treaty allies.

Space Security and Allies

**U.S. Allies in Space**

According to a 2021 study by U.S. Air University, fifteen of the 29 NATO allies operate 384 satellites. While the United Kingdom operates the most satellites (131), it is France that has the most military satellites (14) in orbit. In comparison, there are 1,425 U.S. satellites in orbit by the time of this study. NATO allies also contribute to space domain awareness through ground stations. The European Union consists of all European NATO member states and other non-NATO states and is expanding its presence in space, too. For example, the EU’s space-based PNT service, Galileo, is close to reaching its full operational capability.

Japan, one of the closest allies to the United States in the Indo-Pacific region, has an extensive space program and currently operates sixty-eight satellites in orbit (including one military communication satellite.
and ten spy satellites). It has developed heavy-lifting launch capabilities and fielded the regional PNT service known as QZSS. Its commercial space industry is also burgeoning. To defend its growing space activities from threats, Japan announced the establishment of a Space Operations Command in 2019 and a Space Operations Squadron in 2020. The Japanese government subsequently launched the second Space Operations Squadron in 2022.

South Korea is an emerging space power as it became the latest country to successfully launch its homegrown rocket into orbit in 2022. It currently operates 12 satellites (including one military communications satellite) and plans to launch more intelligence, surveillance, and reconnaissance (ISR) satellites to monitor North Korea’s military activities. Recently, the new administration in Seoul unveiled its ambitious plan to reach the Moon by 2032 and Mars by 2045. South Korea also successfully placed a lunar orbiter that will contribute to the U.S.-led Artemis mission.

It is important to note that although these U.S. allies are gradually progressing in their space capabilities, the allies lack defensive capabilities to protect these space assets from malicious acts. These countries have only a few satellites and backups, having a low level of resiliency. Also, the countries lack active defensive capabilities that can target the threats themselves. France displayed its intent to develop anti-satellite (ASAT) laser weapons, but it is still at an early stage of development. The United Kingdom, France, and Japan have latent direct-ascent ASAT (DA-ASAT) capabilities with its ballistic missile programs but never tested them.

**Threat Environment**

U.S. adversaries such as China, Russia, Iran, and North Korea are expanding counterspace capabilities that threaten United States and allies’ space infrastructure. The People’s Republic of China (PRC) has demonstrated an array of counterspace technologies from DA-ASAT missiles to co-orbital ASAT capabilities. According to Secure World Foundation, China conducted at least ten DA-ASAT weapons tests from 2005 to 2018. More recently, China deployed GPS jammers to the artificial islands in the South China Sea hampering U.S. naval operations in the region. Its military doctrine also prioritizes space dominance as a key to winning future battlefields. Dean Cheng points out that the PRC is prepared to deter and deny the United States and its
allies through space. Although the PRC has not directly targeted U.S. Indo-Pacific allies in space yet, the country will probably leverage its counterspace capabilities to win geopolitical gains given its aggressive and coercive behavior in other domains such as in the South China Sea and cyberspace. Russia is a traditional space power that inherited the Soviet’s counterspace technologies. Despite its limited space budget, Russia recently conducted a kinetic ASAT test in 2021 and a space-based ASAT capability test in 2020. Russia possesses ground-based lasers that can blind satellites and sophisticated mobile jammers. It has deployed GPS jammers to Syria and Ukraine to counter drones and other GPS-enabled weapons systems. Iran and North Korea also have growing counterspace capabilities. Although they do not have sophisticated space programs like China and Russia, they have developed asymmetrical counterspace technologies to overcome conventional military disadvantages. Both countries similarly took efforts to advance their ballistic missile capabilities and employ GPS and SATCOM jammers.

Experts have suggested diverse scenarios where adversaries use counterspace capabilities to advance strategic interests. Aggressors can gradually escalate the situation by undertaking reversible actions such as jamming first and then resorting to non-reversible actions. For example, a study offers a scenario where Russia first jams all SATCOMs in the Baltics to bolster its sphere of influence and then destroys a defunct satellite. Similarly, Admiral Sir Tony Radakin, the head of British Armed Forces, recently warned that Russia could strike space assets of NATO allies. Cheng and other scholars also discussed the possibility of Chinese aggression in space against the United States and its allies to gain the upper hand in the East and South China Sea. The PRC military planners have written about a step-by-step space escalation strategy ranging from a display of space weapons to “space shock and awe strikes.” Considering the growing counterspace capabilities of United States adversaries and the relative weakness of U.S. allies, the need for effective extended deterrence in space is ever pressing.

United States Policies on Space Extended Deterrence

Ensuring the United States and its allies’ access to space and deterring harmful actions have been one of the U.S. government’s policy priorities. The 2020 Defense Space Strategy states that the Pentagon will be prepared “to protect and defend the United States and, as
directed, allied, partner, and commercial space capabilities and to deter and defeat adversary hostile use of space.”

Furthermore, the Biden Administration puts forward the concept of integrated deterrence which “entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and U.S. network of alliances and partners.” Through integrated deterrence, Washington seeks to dissuade its adversaries not only from launching nuclear strikes or large-scale conventional attacks but also from aggressive behavior that falls short of war but still threatens the security interests of the United States and its allies.

The United States also continues to broaden space cooperation with its allies and strengthen extended space deterrence. NATO adopted a new space policy in 2019 and declared space an operational domain. More significantly, at the 2021 Brussels Summit, the leaders of the alliance acknowledged that “attacks too, from or within space present a clear challenge to the security of the Alliance and could lead to the invocation of Article 5 of the North Atlantic Treaty.” However, “a clear challenge to the security of the Alliance” has not been clearly defined. Similarly, the United States and Japan adopted the 2015 Guidelines for Japan-U.S. Defense Cooperation which states that “the two governments will take measures to ensure Japan’s peace and security in all phases, seamlessly, from peacetime to contingencies.”

This was a quantum leap from the previous guidelines from 1978 and 1995 which only discussed scenarios involving a traditional armed attack situation. The 2015 Guideline also included a separate section entitled “Space and Cyberspace Cooperation” which reaffirmed that the United States would assist Japan if its space-based assets are threatened. Moreover, the two governments established the Space Cooperation Working Group to deepen their defense cooperation in space. Lastly, Washington and Seoul are also making efforts to bolster their space cooperation. In 2011, the Joint Communique of the 43rd Security Consultative Meeting—the annual meeting between the U.S. Secretary of Defense and the Korean Minister of National Defense—mentioned the need to strengthen cooperation in the cyber and space domain for the first time. Subsequently, the two governments launched the bilateral Space Cooperation Working Group in 2013 and conducted their first senior-level tabletop exercise for space cooperation in 2017. Furthermore, the U.S. forces in Korea plan to host a U.S. Space Force component command in the future to counter the growing threats from North Korea.
Space Extended Deterrence

The previous section illustrated that the U.S. deterrence policy aims to dissuade adversaries from attacking U.S. allies’ space assets. However, just having a policy is not enough to effectively deter enemies. Extended deterrence, like direct deterrence, is a function of capability and credibility. With the ability to project power globally and one of the most advanced counterspace capabilities, there is no doubt that the United States has the capability to impose costs on adversaries in space or other domains if it is willing to take such forceful measures. Nonetheless, it is questionable whether the U.S. government will follow through with its commitments to defend allies’ space assets and infrastructure. In other words, if Russia blows up a guard post in Poland with a missile strike, it is likely for the United States and other NATO allies to respond militarily. It is not clear, however, whether the United States would retaliate forcefully should the Chinese co-orbital strike destroys Japan’s military earth observation satellite. In this section, I examine the unique characteristics of the space domain that render space-extended deterrence unreliable.

First, it is not easy to establish a clear threshold in space, in which a defender can justify its military action against an aggressor. For extended deterrence to work in space, both a defender and an aggressor should have a clear understanding that certain kinds of hostile actions against one’s space assets will trigger a military response. In a conventional conflict, it can be a violation of territorial integrity or a military attack that results in casualties. Establishing such redlines in space is legally and practically challenging as outer space has no borders and is uninhabited. In formulating a response, a defender must consider the principle of proportionality and military necessity, the central tenets of customary international law of armed conflict. Given that satellites are mostly uncrewed, attacks on them can hardly justify the recourse to violence in other domains. Responding in kind is also not a good option because there exists an asymmetry of dependency between U.S. allies and adversaries.48 For instance, countries such as North Korea and Iran are much less reliant on space-based capabilities militarily and economically than South Korea or Japan. Even the PRC maintains a relatively low level of dependency on space platforms compared to other advanced countries.49 Space debris further hampers effective deterrence in space. Any destruction of a space object will create a large amount of debris that can make the space environment...
hazardous for all. Fearing such collateral damage, a state has only limited options for retaliation. Besides the legal limitations, deterrence by punishment in space is also practically inconceivable. It is hard to imagine a country risking its own soldiers to protect assets far away from the Earth. This is even more unlikely if such assets belong to a third country, in case of extended deterrence. As noted above, U.S. strategists like Schelling introduced the concept of tripwire forces to render extended deterrence credible. It was a mechanism to force an outside power, like the United States, to automatically get involved in a conflict that takes place far from the homeland. However, such a solution is inapplicable in the space domain where most assets are uncrewed.

Thus, even though the United States explicitly states that it will honor alliance commitment in space, the adversaries will think of it as a bluff. As such, U.S. adversaries can take advantage of the absence of a clear threshold and take more aggressive actions toward U.S. allies in space. The PRC in the South China Sea is a case in point. Beijing shaped the balance of power in its favor by deliberately remaining below a blurry threshold in the South China Sea. China has employed paramilitary forces and tactics to expand its influence there. China’s fishing militia forces, also known as “little blue men,” are armed and move in large numbers, driving out other states’ vessels and forming exclusive areas of control. According to Derek Grossman and Logan Ma, Beijing understands that the use of maritime militia is “far less likely to trigger U.S. intervention” even when the threatened party is a U.S. ally. As a result, China built 12.8 million square meters of new land in the South China Sea. From its bases on the artificial islands, it can project its power and deny external intervention in the region more easily. The PRC can employ similar tactics in space by pushing out U.S. allies’ space assets and creating “a zone of non-interference.”

Second, extended space deterrence is challenging due to the difficulty of accurate and prompt attribution. To make deterrence by punishment work, it is crucial for a state to swiftly identify an attacker so that it can retaliate in time. It is not difficult to recognize and attribute movement and attacks of ground, naval, and air units to a state. Even when a country tries to disguise its units, such deception cannot last long—as was the case in Russia’s little green men in Crimea. On the contrary, it is difficult to attribute an attack in space, because of its sheer vastness and the distance between the Earth and satellites. Despite the U.S. Space Force and its allies’ efforts to enhance space domain awareness,
their space surveillance capability is limited. Such limitation hampers the allies' ability to promptly attribute an attack. Also, there is a multitude of space actors. While only a handful of countries could launch and operate satellites decades ago, now more than eighty countries operate their satellites in space and 11 countries can place satellites into orbit. Furthermore, numerous private companies are now present in outer space, too. Locating a responsible party in such congested orbits in a brief time could be a tall order for the still-nascent Space Force. Lastly, space is an “exceptionally harsh environment,” in which natural phenomena such as solar flares or inadvertent interference such as equipment malfunction can cause unintended interferences. Space environments presents potential aggressors with plausible deniability to disguise their intentional attacks and avoid retaliation. In this context, it will be immensely challenging to locate the origin of the attack in space, especially if an aggressor employs non-kinetic capabilities such as jamming or lasing.

Murky attribution is also one of the defining characteristics of the cyber domain where the U.S. government is likewise having trouble deterring adversaries. There, malicious actors deliberately conduct false-flag operations to mislead attribution investigations. For instance, Russia-based groups had tried to shift the blame to the Chinese and North Koreans by planting their codes and malware. United States’ adversaries can emulate a similar strategy in the space domain and further constrain the United States from taking decisive actions to protect its allies in space. If is less confident about committing an aggressive act against its allies, it will be more hesitant in taking actions that might spark inadvertent escalation. The recent controversy of a missile strike on Poland demonstrates the importance of accurate attribution for triggering collective defense obligation.

The distinctive characteristics of the space domain such as uninhibitedness, vastness, and muddy attribution aggravate the problem of credibility that is already salient in extended deterrence. Some might argue that under integrated deterrence, the United States can employ more tailored measures to deter adversaries in space. However, it is extremely difficult to inflict prohibitive pain on adversaries with non-military measures. James Lewis asserts that “ruling out a nuclear response limits deterrence. Anything less than an existential threat or a threat against truly vital interests will not have a deterrent effect.” The failing deterrence in the cyber domain illustrates this point. The U.S. government used an array of non-
military tools such as diplomatic protest, economic sanctions, and indictment to deter malicious cyber acts, but none succeeded to change the cost-benefit calculus of the adversaries.

Others might argue that extended deterrence is built mainly for deterring nuclear and large-scale conventional attacks—also known as “strategic threats”—that United States policymakers should not attempt to deter insignificant threats. Responding to every minor incursion that does not meet the traditional threshold of armed conflict can “cheapen the currency.” Indeed, the core objective of United States extended deterrence was to deter a nuclear attack or large-scale invasion during the Cold War. Nonetheless, this argument fails to account for the significance of the role space plays in military operations in other domains. It is difficult to draw a clear line between strategic threats and non-strategic threats in space since space-based platforms enable and support military systems ranging from ballistic missile early warning sensors to precision-guided missiles. Also, the PRC and other adversaries employ counterspace capabilities in conjunction with military operations in other domains, hence the United States and its allies have the incentive to deter them in space first.

Conclusion

There is a growing need for the provision of extended space deterrence for U.S. allies given the countries’ increasing reliance on space assets and the mounting counterspace threats from adversaries. Although the U.S. deterrence policy affirms that Washington is committed to extending deterrence to its allies in outer space, U.S. adversaries might find such a threat of retaliation not credible. The threat is not convincing because there exists ambiguity in determining a threshold for a military response and difficulty in formulating a response that is both proportional and costly for an aggressor. Second, prompt, and accurate attribution in space poses a significant challenge, hindering the United States to take decisive action on behalf of its allies. Thus, U.S. adversaries are undeterred to take aggressive and assertive actions against U.S. allies in space as they have advanced their geopolitical interests in other contested regions and domains where extended deterrence likewise wanes.

As space security has become an integral part of national security for U.S. allies, policymakers in Washington should also consider extended
space deterrence as one of their priorities. Deterring hostile actions on allies’ space assets serves U.S. national interests as Washington needs strong allies in this emerging domain. Russia’s recent threat to target SpaceX satellites that support operations in Ukraine illustrates the importance of protecting space infrastructure. Given that the traditional logic of deterrence by punishment can be futile in the space domain, the United States might consider putting a greater emphasis on other deterrence mechanisms such as deterrence by denial and deterrence by norm in its extended deterrence strategy. Deterrence by denial of benefit is an apt strategy for the space domain. The U.S. military is already making efforts to bolster its defensive capabilities and resiliency. Furthermore, the recent unilateral moratorium on “destructive, direct-ascent anti-satellite missile testing” by U.S. Vice President Kamala Harris is a good example of building global norms that can restrain potential aggressors’ behavior. By leading global efforts to shape responsible behavior in space, the United States can extend deterrence to its allies and partners, in which space norms can provide a basis for international cooperation to hold those who violate such norms accountable.

Endnotes

13 Schelling, Arms and Influence, 35; Schelling, The Strategy of Conflict, 28.
23 Kevin Pollpeter and Elizabeth Barrett, NATO Ally Contributions to the Space Domain (Montgomery: China Aerospace Studies Institute, 2021).
24 The number of operational U.S. satellites dramatically increased to 3,433 since then, perhaps due to the large constellation built by SpaceX; “UCS Satellite Database,” Union of Concerned Scientists, accessed December 6, 2022, https://www.ucusa.org/resources/satellite-database.

30. Pollpeter and Barrett, NATO Ally Contributions to the Space Domain; Weeden and Samson, Global Counterspace Capabilities.


34. Dean Cheng, Cyber Dragon (Santa Barbara: Praeger, 2017), 165.


40. Cheng, Cyber Dragon, 177.


49. Cheng, Cyber Dragon, 175.


60 Lewis, “Reconsidering Deterrence for Space and Cyberspace,” 68.