A Framework of Deterrence in Space Operations
About This Report

This report presents a framework for understanding deterrence in space operations. There is no broadly agreed-on framework in the U.S. or allied governments or the wider analytic community on the nature and requirements of deterrence in space operations. Concepts of conventional and nuclear deterrence are often applied to assessments of deterrence in space, but these concepts have their limits, given certain unique characteristics of the space domain. The national security and military operations of the United States and many other countries are highly dependent on information derived from and transmitted through space. Over the past two decades, potential adversaries have developed a wide array of increasingly sophisticated means to disrupt or deny the United States and its allies access to their significant advantages in space capabilities. This situation and deepening great-power tensions have given new urgency to assessing the counterspace strategies of potential adversaries and how they can be deterred from taking actions to disrupt or destroy U.S. and allied space assets or be dissuaded from even developing certain counterspace capabilities. In this report, we examine these issues through an analytical framework made up of three archetypes of deterrence in space operations.

This report was originally drafted in October 2020 and slightly updated in December 2022.

RAND National Security Research Division

This research was sponsored by the U.S. government and conducted within the International Security and Defense Policy Program of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

We are grateful to many individuals at the RAND Corporation who supported the development and publication of this research. This project was developed and executed in the former Cyber and Intelligence Policy Center of NSRD, under Richard Girven, director; Sina Beaghley, associate director; Norma Ockershhausen, research finance administrator; and Katrina Doss-Owens, administrative assistant. The report was published under the International Security and Defense Policy Program of NSRD, with support from Michael McNerney, Jim Mitre, Michael Spirtas, and Libby May, as well as from Bruce McClintock, lead of the RAND Space
Enterprise Initiative. The manuscript benefited from insightful peer reviews by Frank Klotz, adjunct senior fellow, and Karl Mueller, senior political scientist, both at RAND. We are also very grateful to Cecile St. Julien for her support during the planning and execution of the research, Allison Kerns for superb efforts in editing, and Emily Ward for finalizing the report.
Summary

Issue

The national security and military operations of the United States and many other countries are highly dependent on information derived from and transmitted through space. Over the past two decades, potential adversaries have developed a wide array of increasingly sophisticated means to disrupt or deny the United States and its allies access to their significant advantages in space capabilities. This situation and deepening great-power tensions have given new urgency to understanding the counterspace strategies of potential adversaries and how they can be deterred from taking actions to disrupt or destroy U.S. and allied space assets or be dissuaded from even developing certain counterspace capabilities. Aspects of this topic have been addressed in many excellent studies and reports. However, there is no broadly agreed-on framework in the U.S. and allied governments or the wider analytic community on the nature and requirements of deterrence in space operations. Concepts of conventional and nuclear deterrence are often applied to assessments of deterrence in space, but these concepts have their limits, given certain unique characteristics of the space domain.

This report seeks to fill this analytic gap by presenting such a framework, which is comprised of three archetypes for deterrence in the space domain that can be utilized to identify and assess the deterrence strategies of various countries and illuminate how a nation could deter disruptive or destructive attacks on its space assets.

Approach

We begin with a review of the canonical and more-recent scholarly literature on deterrence and identify several foundational principles of deterrence. We then consider what lessons deterrence in other domains—nuclear and cyber—have for deterrence in space. We next examine the nature and requirements of deterrence in the space domain, what constitutes success in space deterrence and thresholds of deterrence failure, and selected national approaches to space deterrence—China, Russia, France, Japan, and India. Finally, we present three archetypes for...
space deterrence and consider several questions about the application of deterrence under various circumstances.

Findings

Relevance of the Foundational Principles of Deterrence for Space

The concept of deterrence is receiving renewed attention from strategists and defense planners as a result of growing great-power competition and other developments in the global security environment. This competition extends across all domains and increasingly involves informational and other nonkinetic activities below thresholds that would trigger robust military responses. As a consequence, the foundational principles of and approaches to deterrence that evolved during the Cold War are being adapted, with implications for deterrence in the space domain.

There are two main strategies for achieving deterrence:

- **Denial.** In a denial strategy, by demonstrating the capacity and will to defeat an adversary’s attack or render it ineffective, a nation aims to convince an adversary that it will be unable to achieve its goals militarily.
- **Punishment.** In a punishment strategy, by threatening a potential attacker with severe consequences, a nation aims to convince the adversary that the objectionable action or aggression has unacceptable costs.

Both of these strategies are relevant to space, and mixtures of the two approaches are also possible.

Assurances, including incentives or concessions for forsaking aggression; declarations about the scope and limits of a country’s responses to aggression; and offers of potential off-ramps to de-escalate a conflict also play a role in influencing a potential challenger’s cost-benefit calculus and may have utility in deterring or terminating counterspace actions.

Dissuasion is another element of strategy relevant to preventing aggression in space. This strategy seeks to prevent the emergence of a threat by convincing another actor that developing certain menacing capabilities or even initiating a military competition would be futile.

The Chinese concept of *weishe* combines the Western concepts of deterrence and compellence, seeking to convince an opponent to refrain from a particular action and submit “to the deterrer’s volition.”

Three aspects of stability are also relevant to assessing the requirements of deterrence in space: strategic stability, crisis stability, and arms race stability.

Lessons of Nuclear and Cyber Deterrence

Nuclear deterrence theory and practice offer five central concepts that can be leveraged to build a framework for deterrence in space: credibility, deterrence stability, the inversion of offense and defense, crisis stability, and escalation.
Credibility is the cornerstone of nuclear deterrence. It means that the deterring state is perceived to have the will to retaliate with nuclear weapons if it or an ally is attacked.

Nuclear and space deterrence both have an inversion of what constitutes an offensive and defensive attack; however, there is no analogue in space warfare for an assured second-strike capability.

The challenges associated with deterring cyberattacks often parallel those for deterring space asset attacks; such challenges can include attribution, credibility, proportionality of response, and the ability to control escalation.

Because cyber and space attacks will likely have mostly material and economic effects rather than a human toll, threats to retaliate may be viewed as disproportionate, escalatory, and incredible. Responding to such attacks requires carefully calibrated retaliatory actions, though not necessarily in kind.

**Key National Perspectives on Space Deterrence**

There is no consensus definition of space deterrence among the international community. Various countries have quite different conceptions of what the term means and how it can best be achieved.

**China’s** concept of space deterrence refers to the threat or actual limited use of force in space, supported by powerful counterspace forces, to curb an adversary’s military operations. Space deterrence operations are not necessarily or exclusively designed to deter actions in the space domain. Because space deterrence is “strategic, convenient, and controllable,” Chinese strategists contend that it has become the principal, more frequently used form of military deterrence. To enhance deterrence, China has an operational concept of gradual escalation in space operations, culminating with attacks on adversary space systems.

**Russia** views space as a warfighting domain and posits that U.S. reliance on space creates an Achilles’ heel that presents Moscow with a variety of opportunities to obtain its objectives and prevail in a conflict. Russia has developed a counterspace doctrine designed to deter aggression and, should deterrence fail, control escalation through selective targeting of adversary space systems. Russian doctrine envisions employing various ground-, air-, and space-based systems to disrupt or destroy adversary spacecraft and supporting infrastructure. Russia’s so-called Strategic Operations to Destroy Critically Important Targets strategy is intended to employ metered levels of damage to seize or retake the initiative and includes striking communication nodes and space surveillance systems.

**France’s** Defence Space Strategy seeks to ensure the country’s freedom of decision and action in space and involves efforts to integrate improved space situational awareness capabilities, passive and active defense measures to avoid or dazzle hostile space systems, and limited reconstitution capabilities. France maintains that its space strategy is designed to enhance self-defense capabilities.
Japan has no declared offensive counterspace capabilities. Its Space Operations Squadron, formed in 2020, has a mission to provide “persistent monitoring.” However, the Japan Self Defense Force has announced that, to “ensure superiority in use of space at all stages from peacetime to armed contingencies,” it will implement mission assurance measures and its capability to disrupt opponents’ command, control, communications, and information capabilities.

India framed its March 2019 destructive antisatellite weapon test Mission Shakti as being designed to bolster space deterrence in the face of growing threats to the country’s space systems, and some officials said that the generation of debris was required to demonstrate a credible counterspace capability.

Success and Failure in Space Deterrence

The central goal of space deterrence is to prevent or limit nonkinetic and kinetic attacks against satellites and space support systems that would destroy those assets or significantly disrupt their operations. The success of space deterrence is not binary. It should be measured along a spectrum that takes into account differing requirements for space services at various phases of a conflict and in light of how the conflict is unfolding in other domains.

The prospects for complete success in deterrence of hostile attacks on space assets, particularly reversible, nondestructive attacks, are limited. Reversible attacks are the most difficult to deter because adversaries assess that they have lower risks of a robust response or escalation.

A space deterrence strategy focused on mitigating damage and preserving essential capabilities through a mix of defensive and offensive counterspace actions, resilience measures, and reconstitution is most likely to be successful.

Framework for Deterrence in Space

Drawing on the foregoing analysis, we present a framework for assessing the deterrence approach being pursued by any country. We present the framework as three archetypes for space deterrence:

1. Denial dominant: Deterrence that relies primarily on resilience, stealth capability, defensive measures, and redundancy to convince an adversary that it would be unable to achieve a decisive advantage by attacking the target country’s space systems. This strategy may include some active defenses but limited capability to degrade the space systems of other countries. This approach also seeks to regulate the use of force in space through norms and sanctions for bad behavior.

2. Mixed deterrence: Deterrence achieved by a mix of resilience and defensive measures, combined with robust active defenses of space assets and more-substantial capabilities to degrade the space systems of other countries. This approach also sees merit in trying to regulate the use of force in space through norms and sanctions for bad behavior.
3. *Offense dominant*: Deterrence that includes elements of denial and resilience but relies more on punishment. This approach places emphasis on a variety of counterspace weapons capable of severely degrading the space systems of other countries, possibly combined with the threat of debilitating responses in other domains. This approach is designed to convince an adversary that it has much more to lose in attacking another country’s space systems, because any threat of or actual attack will result in robust counterspace actions. Norms are not a priority for states with this posture because they do not trust most other spacefaring nations to uphold them.

None of the three archetypes appears more predisposed to success or failure than the others. A comprehensive approach to space deterrence—one that seeks to regulate the use of force in space in the interest of stability; ostracizes states that violate agreed-on norms; and allows states to retain some capacity to punish space aggressors in multiple domains and to develop measures to enhance the defenses, resilience, and redundancy of space systems—may have the greatest probability of success. Cross-domain influences and interdependencies affect the success and failure of each archetype. Nevertheless, these archetypes provide a useful framework for assessing the strategy and goals of various countries in the conduct of their space operations and illustrating how a nation can deter attacks on its space assets.

The underlying informational needs—and how well each side is postured to meet these needs—will also influence the choice of deterrence methods. Strategic messaging and deliberate revelation of selected space capabilities, as well as how various approaches to space deterrence support or conflict with other forms of deterrence, further influence deterrence. An effective space deterrence strategy should be tailored to address the distinct risk calculus of various adversaries across the phases of conflict (peacetime, competition, crisis, and conflict).
Contents

About This Report ......................................................................................................................... iii
Summary .......................................................................................................................................... v
Tables ............................................................................................................................................. xi
Chapter 1. Foundational Principles of Deterrence ................................................................. 1
  Defining Deterrence ..................................................................................................................... 2
  Tailored Deterrence .................................................................................................................. 4
  The Role of Assurance .............................................................................................................. 5
  Dissuasion ................................................................................................................................. 5
  The Chinese Concept of Deterrence ......................................................................................... 6
  Other Factors Affecting Deterrence: Stability, Context, Phasing ............................................ 7
Chapter 2. Lessons from Other Domains: Nuclear and Cyber ................................................. 10
  Nuclear Deterrence .................................................................................................................. 10
  Cyber Deterrence ..................................................................................................................... 15
Chapter 3. Defining Success in Space Deterrence ................................................................. 18
  What Is Space Deterrence? ...................................................................................................... 19
  Measures of Success .............................................................................................................. 20
  Impediments to Success ......................................................................................................... 21
  Selected National Approaches to Space Deterrence .............................................................. 22
  Measuring Success and Comparative Strategies for Space Deterrence ............................... 28
Chapter 4. Framework for Deterrence in Space .................................................................... 30
  Archetypes of Space Deterrence .............................................................................................. 30
  Elements For Space Deterrence Analysis .............................................................................. 32
  Situational Considerations Affecting Outcomes .................................................................. 33
  Possible Contribution of Norms ............................................................................................. 36
  Impact of Messaging and the Revelation of Capabilities ......................................................... 37
  Cross-Domain Considerations ............................................................................................... 38
Abbreviations .............................................................................................................................. 40
References ..................................................................................................................................... 41
Tables

Table 4.1. Elements of the Three Archetypes of Space Deterrence ..............................................31
Table 4.2. Elements of Deterrence in the Space Domain, by Archetype ........................................33
Chapter 1. Foundational Principles of Deterrence

The concept of deterrence, a foundational element leveraged by U.S. defense planners to manage superpower competition during the Cold War, is receiving renewed attention from strategists and defense planners given several developments in the global security environment. The three decades since the end of the Cold War—characterized by U.S. military predominance, limited regional conflicts, and counterterrorism campaigns—have given way to an era of renewed great-power competition. As countries have moved to challenge U.S. predominance, this competition has become more intense across all domains and increasingly involves informational and other nonkinetic activities below thresholds that would trigger robust military responses. The space domain has become more competitive as the number of countries and commercial entities utilizing sophisticated space systems has grown dramatically. Moreover, the potential for the initial stages of future conflicts to originate in outer space, or for terrestrial conflicts to extend there, has grown as both major and medium powers seek to level the playing field or gain asymmetric advantage against potential adversaries. The June 2020 U.S. Defense Space Strategy Summary notes two related challenges to achieving the United States’ long-term objectives that space remain secure, stable, and accessible; these challenges are relevant to all current space-faring nations:

- The U.S. Department of Defense has limited operational experience with conflict beginning in or extending into space, despite rapid counterspace advancements by potential adversaries.
- International understanding and agreement of what constitutes unsafe, irresponsible, or threatening behavior in space is nascent.²

All these factors created a new urgency to better understand what deters attacks on space systems. Our analysis seeks to fill this gap by developing a framework of archetypes that can be applied to help policymakers and military planners assess the space deterrence approach being pursued by any country. As a first step in conceptualizing this framework, the next chapter reviews the foundational principles of deterrence that evolved in the United States during the Cold War, how they are being adapted in the context of today’s more complex security environment, and their implications for deterrence in the space domain.

Defining Deterrence

Western strategists define deterrence, in general, as the process of convincing another actor that the costs or risks of a possible action outweigh the benefits. Deterrence is distinct from what Thomas Schelling called compellence, in which one actor seeks to force another actor to do something or cease an action that it has already undertaken. Deterrence and compellence are forms of coercion; the central distinction between the two concepts is whether the targeted action is being contemplated or has already begun. Deterrence tends to be indefinite in its timing and is designed to convince an opponent to refrain from an offending action. Compellence, on the other hand, prioritizes the actual use of force and comes to the fore in the wake of an adversary nonetheless taking an offending action. To be effective, deterrence and compellence threats must be clearly communicated, specify the demanded outcome, and include a credible commitment of restraint if those demands are met. Note that, for both concepts, one is attempting to alter the behavior of an actor still able to launch an organized military resistance; that is, the adversary is not a defeated, defenseless victim.

A unique characteristic of deterrence, though, is its reliance on the manipulation of the psychological, not the physical. The deterrence literature suggests that, to influence an adversary’s decision calculus, an actor attempts to use deterrence threats to affect two levers: the expected costs and the perceived benefits of the action. Deterring an adversary broadly requires at least one of the following conditions: (1) increasing the anticipated costs of the action, (2) increasing the certainty that these costs will be incurred (retaining the capacity for and conveying the will to undertake a credible response), (3) reducing the anticipated probability that the action will succeed, and (4) increasing the benefits of restraint.

The scholarly literature has identified two distinct strategies to pursuing deterrence: denial and punishment. In a denial-based deterrence strategy, by demonstrating the capacity and will to deny an adversary’s military objectives or render its military strategy ineffective, a nation aims to convince the adversary that it will be unable to achieve its political goals by force. Denial strategies operate by increasing the risk that the adversary’s military strategy will succeed and

---

3 Note that, because deterrence is a process, it should be logically conceived of not as a strategy to be achieved but rather as a strategy to be pursued. The authors thank Courtney Stewart for emphasizing this distinction.


decreasing the likelihood that it will be able to control the objectives in dispute (even if the strategy does succeed). The credibility of deterrence by denial is often measured in the proximate balance of military forces and the effectiveness of defensive countermeasures.\(^8\) In the space domain, this could include a mix of resilience measures, active defenses, and offensive counterspace capabilities to deny an adversary use of systems that threaten space-based assets. The interest in deterrence-by-denial strategies has been revived by Russia, China, and other countries’ growing use of “gray-zone” and limited-war techniques that seek to operate below the threshold that would trigger a robust military response.\(^9\)

\textit{Punishment}-based deterrence strategies operate by threatening costs that are greater than the value of the objective that the challenger seeks to gain.\(^10\) Punishment strategies threaten further escalation of violence and imposition of wider costs away from the main battle front, for example, economic sanctions or attacks on industrial assets and civilian populations. In the space context, punishment could include actions to damage or destroy space-based systems, disrupt an adversary’s economy, or military actions against the civilian sector in other domains. The public exposure of actions that are taken that run counter to widely accepted norms can also be used to enhance deterrence by punishment—i.e., naming and shaming. U.S. officials believe that the Chinese government has refrained from debris-creating anti-satellite tests over the past 16 years, in part, as a result of the international opprobrium directed at Beijing following its 2007 destruction of a defunct weather satellite using a ground-based medium-range ballistic missile, which created thousands of new pieces of space debris.\(^11\)

Deterrence could also be pursued using a mixture of denial- and punishment-based threats.\(^12\) The primary conclusion of extensive game theoretic analysis of space warfare incorporating prospect theory,\(^13\) conducted by Bonnie Triezenberg, is that “how nations feel about their


\(^13\) Prospect theory is a behavioral economics model based on the observation that, although humans like to win, they more strongly prefer not losing.
standing under the status quo has a larger effect on outcomes than any of the rational factors I studied.” Triezenberg’s analysis concluded that the best strategy “to deter debilitating attacks on space systems is to ensure that opponents in any future conflict feel they have ‘something to lose’ if that war were to expand into outer space.”

One can imagine a strategy that employs a mixture of denial- and punishment-based threats to increase the likelihood that opponents perceive that they have something to lose, e.g., manipulating reliance on global positioning systems or weather satellites.

The circumstances within which deterrence can be pursued vary along with the strategies. First and foremost, states leverage deterrence strategies in an effort to preclude attacks within their territorial boundaries and on national interests abroad. In the context of alliances and other security commitments, deterrence can, theoretically, also be extended. Thus, states can also leverage deterrence strategies to try to dissuade attacks on the territory of their allies or partners. Extended deterrence is presumed to be more difficult objective, though, as it presents additional challenges. Not only must a state have the capability to project power and carry out such threats, but it must also be perceived to have the will to do so, which can be uncertain. As was often debated during the Cold War: Would a state otherwise unharmed really risk its blood and treasure for a third party? And would that third party have confidence in this commitment? Extended deterrence threats consequently present a unique credibility problem. Because the space domain is outside the territorial boundaries of the United States and does not present the risk of citizen casualties, among other features, deterring aggressive actions in space may thus look and behave more like extended deterrence than direct deterrence. This point is discussed in more detail later in the report.

**Tailored Deterrence**

In the early 2000s, strategists recognized that the concepts of deterrence that had evolved during the bipolar competition between the United States and the Soviet Union and their respective allies needed to be adapted to a more complex international system. The 2006 U.S. Quadrennial Defense Review outlined an approach of “tailored deterrence” to address the diverse challenges posed by the emergence of several advanced military competitors, regional powers armed with weapons of mass destruction, and nonstate terrorist networks. In developing this approach, U.S. strategists contended that tailored deterrence requires detailed assessments of the leadership and society that one seeks to influence. With this information, one can integrate a

---


15 Mazarr, 2018, p. 3.

variety of military, diplomatic, informational, and economic instruments to tailor one’s
deterrence approach to a particular context and adversary. Tailored deterrence also requires clear
and credible messaging and a mechanism to assess how statements and actions are perceived (or
misperceived) and how they affect an adversary’s decision calculus.17

The 2018 U.S. Nuclear Posture Review (NPR) elaborated an approach for tailoring
deterrence to a variety of potential adversaries with differing interests, strategies, and military
capabilities in various circumstances and for communicating the costs of aggression in ways that
take into account each adversary’s unique risk calculus. The NPR articulated tailored deterrent
strategies toward Russia, China, North Korea, and Iran and called for a diverse mix and range of
options to deter one or more potential adversaries in different circumstances.18

Given that states have differing degrees of reliance on space (whether enabling military
operations or commercial operations, or both) and differing capabilities for holding space-based
assets at risk or protecting their own assets, one can imagine the utility of tailored deterrence
strategies in the space domain.

The Role of Assurance

The classical deterrence literature also notes the delicate balance to be struck between having
forces and policies sufficient to deter while also taking care not to trigger security dilemma
dynamics. Actions taken to increase the security of one state can decrease the security of another,
leading to arms racing and, potentially, conflict that leave both sides worse off.19 Moreover,
threats are often insufficient for deterrence to succeed, and assurances play a role in influencing a
potential challenger’s cost-benefit calculus. Thus, measures taken to demonstrate restraint—to
assure the adversary that their restraint will accrue benefits—have crucial utility in deterring
conflict. Assurances can include incentives or concessions for forsaking aggression, declarations
about the scope and limits of a country’s responses to aggression and offers of potential off-
ramps to de-escalate a conflict.20

Dissuasion

The final strategic element relevant to framing thinking about conflict in the space domain is
dissuasion. Dissuasion does not seek to convince another state to avoid aggression. Rather, the

and Mazarr, 2018, p. 5.
intent is to influence or shape the behavior of that state to prevent the emergence of a threat. Dissuasion aims to convince another state that developing certain threatening capabilities or initiating a military competition would be futile. Dissuasion is generally seen as a peacetime activity involving an array of nonmilitary and military activities. Dissuasion is thus sometimes characterized as “pre-deterrence” or as a form of deterrence by denial. Paul Davis argues that dissuasion can be more effective if combined with elements of deterrence by punishment and other mechanisms to impose cost.

Dissuasion was a major feature of the Ronald Reagan administration’s strategy in the 1980s. The strategy was leveraged to convince the Soviet Union that it could not win an arms race, given superior U.S. technological and economic strengths. So, too, the 2001 U.S. Department of Defense Quadrennial Defense Review asserted that U.S. research, development, test, and demonstration programs, along with maintenance or enhancement of advantages in key areas of military capability can “dissuade other countries from initiating future military competitions.”

The 2018 U.S. National Strategy for Space and the 2020 Defense Space Strategy Summary reflect elements of dissuasion, calling for achieving superiority in space—defined as being able to conduct U.S. operations without prohibitive interference from adversary, while simultaneously denying an opponent freedom of action in the domain for a period of time—and maintaining that superiority through the development and acquisition of critical space systems. The first U.S. Space Force Space Capstone Publication (SCP), Spacepower, makes a further distinction between space superiority and “space supremacy,” defining the latter as one side having the ability to conduct operations with relative impunity while denying freedom of action in the space domain to an adversary. The SCP concludes that “space supremacy is not always desirable, or attainable against a peer adversary, and should not be the unconditional goal of military spacepower.”

The promulgation of both concepts represents a form of dissuasion.

The Chinese Concept of Deterrence

Of course, the West does not have a monopoly on thinking about deterrence. Chinese approaches to deterrence and dissuasion differ noticeably from Western concepts. Chinese strategists see deterrence as a means to achieve wider strategic objectives rather than strictly an

---

23 Davis, 2014, p. 5.
approach for protecting national interests, conflict avoidance, and strategic stability.27 The Chinese term *weishe*, generally translated as *deterrence*, combines the Western concepts of deterrence and compellence and is thus closer to Schelling’s original concept of coercion, with a clear recognition of the psychological component.28 Strategic *weishe*, according to the authoritative 2001 *Science of Military Strategy*, has two roles: “one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and both demand the opponent to submit to the deterrer’s volition.”29 Given this dual purpose and broader Chinese revisionist efforts to change numerous unfavorable ‘status quos’ it confronts over time, China’s concept of deterrence also has some similarities with the Western concept of dissuasion. Chinese concepts are discussed in more detail in Chapter Four of this report.

Other Factors Affecting Deterrence: Stability, Context, Phasing

Three variants of stability—strategic stability, crisis stability, and arms race stability—are also relevant to assessing the requirements for deterrence. In addition, another factor affects the likelihood that deterrence strategies will be effective: the context within which they are pursued, or the phase within which they are operating (peace, competition, crisis, or conflict).

In their early analysis of deterrence in the 1950s, Thomas Schelling and Bernard Brodie explained that the symmetry or asymmetry of offensive power between antagonistic nations is less important than the stability of the balance of power between them. Brodie and Schelling hypothesized that an unstable balance of power arises when one side can destroy the other’s capacity to retaliate by striking first. As Brodie noted, “Stability is achieved when each nation believes that the strategic advantage of striking first is overshadowed by the tremendous costs of doing so.”30 Although this construct was proposed to characterize stability in a nuclear context, it has intuitive relevance in a conventional context as well. In the literature on nuclear deterrence,

---

27 For one overview, see Dean Cheng, “Chinese Views on Deterrence,” *Joint Force Quarterly*, No. 60, 2011.
the retention of an assured second-strike capability was seen as the essential enabler of strategic stability and the sustainment of mutual deterrence.

However, scholars have noted that even under conditions of strategic stability, amidst a crisis in which conflict seems imminent and inexorable, a government concerned that its deterrence forces are vulnerable to a first-strike might be driven to a preemptive strike for fear of “use-it-or-lose-it” dynamics. Crisis stability is seen to hold when antagonists assess that there is limited risk of preemptive strike that would degrade either side’s ability to inflict significant damage in retaliation. Crisis stability in the nuclear era has thus been seen as reducing the risk of preemptive, inadvertent, or accidental nuclear war. If antagonists are developing weapons or modernizing their forces in ways that would create such a preemptive capability—i.e., a capability that would preclude their adversary from retaliating—such developments could threaten to undermine strategic or crisis stability. Finally, arms race stability is a condition in which antagonists are less concerned that the other side’s build up of arms provides a military advantage that threatens strategic or crisis stability.

In the space domain, strategic and crisis stability could be undermined if one side perceives that (1) attacking an opponent’s space assets offers a strategic advantage or (2) an opponent possesses decisive counterspace capabilities. Authoritative Chinese military texts reflect the former situation; they imply China’s plans to pursue what Western governments could perceive as preemptive strikes against space systems. Yet such a strategy should be expected, given the conventional military advantages accrued by the United States from its space assets. Strategic and crisis stability could still be reinforced, though, through a variety of mechanisms, including the development of resilient space architectures, redundancy, effective defenses, and reconstitution capabilities.

Finally, the context within which deterrence is practiced can vary. Specifically, depending on the phase of the conflict—peacetime, competition, crisis, or conflict—the approach to deterrence may change. The term general deterrence is used to describe long-term efforts to discourage hypothetical attacks in peacetime and the competition phase. General deterrence therefore principally relies on one’s overall military posture and the impression that it projects.

Immediate deterrence, on the other hand, pertains to active crises and efforts to discourage a

---


specific, imminent attack and maintain stability. In this context, deterrence principally relies on specific military capabilities proximate to the relevant theater of crisis or conflict and the threats made credible by those capabilities.\textsuperscript{35} Both the overall military posture and specific military capabilities can be leveraged within the context of an actual conflict to produce intra-conflict deterrence—for example, by deterring an adversary from using certain types of weapons or escalating the intensity or scope of the conflict.\textsuperscript{36}

Previous analysis by Forrest Morgan highlighted the interdependence between general deterrence and space deterrence. Given U.S. reliance on space, if adversary leaders assess that attacking U.S. space systems would degrade overall U.S. warfighting capabilities sufficiently to realize the adversary’s objectives in a conflict at acceptable costs, general deterrence would be eroded. Conversely, if those same leaders assess that attacking U.S. space systems presented unacceptable risks of conflict escalation—i.e., escalation to the nuclear threshold—deterrence in the terrestrial domain would be reinforced by the knowledge that U.S. military forces would be operating with the full benefit of support from space-based assets. This calculus would apply to other countries with significant space assets. As Morgan noted, “In sum, effective space deterrence fortifies general deterrence and stability.”\textsuperscript{37}

Each concept discussed above is pertinent to developing a framework for deterrence in space, assessing military postures and policies required to deter and dissuade hypothetical attacks, and identifying the specific capabilities and policies most likely to persuade an adversary to avoid escalation in a crisis or a conflict. Before we turn to that framework in Chapter Four, we consider lessons that the nuclear and cyber domains may have for space deterrence (Chapter Two) and outline what would constitute success in space deterrence (Chapter Three).

\textsuperscript{35} Morgan, 2003, p. 81; and Mazarr, 2018, p. 4.


\textsuperscript{37} Morgan, 2010, p. 21.
Chapter 2. Lessons from Other Domains: Nuclear and Cyber

Deterrence in the nuclear and cyber domains offers useful parallels but also differs from that in the space domain. Each of these domains has distinct characteristics that limit the scope for broad generalizations, but exploring the principles of each and their differences is instructive. This chapter discusses what lessons from, and experience in, these two domains may usefully be leveraged in crafting a framework for space deterrence. Furthermore, it considers how interactions across all three domains plausibly affect overall stability, crisis stability, and crisis management.

We begin the discussion with nuclear deterrence, because so much of classical concepts of deterrence are rooted in the development of nuclear strategy. We then proceed to consideration of the cyber domain, which also provides useful framing given that the challenges associated with deterring cyberattacks often parallel those for deterring attacks on space assets. Such potential challenges include attribution, credibility, proportionality of response, and the ability to control escalation. But cyber warfare also contains some distinct differences from counterspace activities. The growing use of asymmetric “gray-zone” tactics—which are often supported by cyber and space capabilities, as well as other instruments of coercion—by both major and middle-tier powers to achieve strategic goals without the overt use of military force, highlights the need to better understand the linkages among deterrence measures calibrated for these various domains.38

Nuclear Deterrence

Understanding the principles of nuclear deterrence, particularly during a period of deepening great-power competition and the emergence of nuclear-armed middle-tier powers, is central to any consideration of how best to deter conflict in the space domain. The term nuclear deterrence generally refers to the threat or actual use of nuclear weapons to deter aggression. Nuclear deterrence theory and practice offer five central concepts that can be employed to build a framework for pursuing deterrence in the space domain: credibility, deterrence stability, the inversion of offense and defense, crisis stability, and escalation.

Arguably, the differences between nuclear and space deterrence outweigh their similarities. A considered comparison, however, reveals some common characteristics and applicable principles. Moreover, one could look to the extensive literature on the effectiveness of nuclear threats in deterring various forms of aggression. However, we follow Karl Mueller’s approach in

---

38 See Ashley Townshend, David Santoro, and Brendan Thomas-Noone, Revisiting Deterrence in an Era of Strategic Competition, Sydney: United States Studies Centre at the University of Sydney and Pacific Forum, February 2019.
comparing nuclear and space deterrence, hypothesizing it is more instructive to focus on how the use of nuclear weapons has been and can be deterred, either by threats of nuclear response or other means. For this part of the analysis, we are interested in what the nuclear experience might tell us about deterring attacks against satellites and other space systems, not what it might tell us about using space capabilities for wider deterrence purposes.  

Credibility is the cornerstone of nuclear deterrence. The deterring state must be perceived as having the will and capability to retaliate, including with nuclear weapons, if it, or an ally to which it has extended a security guarantee, is attacked. Debate persists, however, regarding what specific capabilities are required for nuclear deterrence to remain stable. One school of thought, consistent with the recommendations of the 2018 U.S. Nuclear Posture Review, reflects the theory that deterrence requires a state to equip itself to fight and win at every level of nuclear conflict for deterrence to prevail. Other schools argue that nuclear deterrence simply requires sufficient armaments to deny an adversary its objectives, which can be achieved with an assured ability to launch a sufficiently painful retaliatory strike. This debate persists because deterrence is psychological, and the deterred must be convinced of the deterrer’s will and capabilities.

A similar disagreement regarding the requirements for nuclear deterrence can already be seen extending to the capability requirements for space deterrence. For example, if an adversary deploys a dedicated anti-satellite (ASAT) missile system, must the targeted government follow suit and be able to launch a strike in kind to successfully deter? Similar “rungs on an escalation ladder,” in the words of Herman Khan, may thus exist in space. Forrest Morgan and his co-authors have argued persuasively that a more appropriate metaphor would be a slippery slope to escalation. They liken calibrating responses to attacks to traversing a dangerous mountainside, with the bottom of the slope representing the most extreme level of escalation. In their analogy, they cast controlling escalation in this way: “Depending on the location of hand- and footholds, descending to greater degrees of escalation may assist one’s progress, or may even be essential to it, but the challenge is to maintain control over this escalatory descent. Carrying this analogy into the space domain, major space-faring nations must wrestle with whether to seek a superior space warfighting capability by deploying a suite of capabilities to disrupt or destroy adversary space assets. Such a strategy, though, could be pursued at the potential risk of causing

adversaries to perceive such a nation is implementing an offensive counterspace doctrine and that war beginning in (or rapidly extending into) space is inevitable.\textsuperscript{44}

Finally, an important difference between the two domains is that, no matter how resilient and redundant a nation’s space and counterspace architecture might be, there is no strong analogue in space warfare for an assured second-strike capability—i.e., there is no parallel guarantee of a devastating reprisal that has consequently stabilizing effects.\textsuperscript{45} Plausibly, though, the capacity of a state to promptly reconstitute its satellites and other space-related systems that are damaged or destroyed by an adversary, together with a capacity for removal or mitigation of space debris, could provide some of the stabilizing benefits akin to an assured second-strike capability. Such a capability to sustain critical space-based assets to support other aspects of national warfighting capabilities—including threatening adversary space systems and orbital ASATs—would make counterspace strikes less effective and possibly less attractive to an aggressor.

Understanding the capabilities required for deterrence stability is essential, because an additional similarity between deterrence in the nuclear and space domains is the inversion of what constitutes an offensive and defensive attack.\textsuperscript{46} Unlike conventional deterrence, threatening to attack an adversary’s nuclear arsenal and deploying defenses to protect one’s cities are both considered to be offense-oriented acts that threaten stability. Alternatively, threatening to attack cities and constructing defenses around one’s nuclear arsenal are defense-oriented acts. The latter are defensive in nature because they do not threaten to undermine the adversary’s ability to retaliate. Space presents a similar inversion of the traditional understanding of offense and defense.\textsuperscript{47} Threatening to attack another country’s satellites, even during overflight of one’s own territory, constitutes an offense-oriented act. Deploying a capability to limit and rapidly clean up space debris generated by a destructive ASAT weapon could also be considered offense-oriented. Such a capability would likely be perceived as building a “shield for the sword,” in the sense that a state might then be able to strike another’s space assets and still be able to protect its own space-based capabilities from the resulting debris.

In addition, the idea of crisis stability within nuclear deterrence theory is also relevant. When a strong incentive exists to strike first, because the perception exists that the side that does so will be much better off, then crises will tend to be less stable, as there will be increased potential for escalation to outright conflict.\textsuperscript{48} Combining surprise, promptness, precision, and sufficient levels

\textsuperscript{44} Morgan, 2003, pp. 25–33; and Krepon, 2013, p. 37. Note that empirical analyses suggest that the requirement for effective deterrence does not need to be an assured ability to win. Mazarr cites the literature to argue that “[a] defender can succeed by deploying sufficient local forces to raise the cost of a potential attack, to make escalation inevitable, and to deny the possibility of a low-risk fait accompli.” See Mazarr, 2018, p. 6.

\textsuperscript{45} Mueller, 2013, p. 56.

\textsuperscript{46} Mueller, 2013, p. 53.

\textsuperscript{47} Mueller, 2013, p. 53.

\textsuperscript{48} Mueller, 2013, pp. 50–51.
of destruction creates a scenario in which the ability to retaliate can potentially be undermined. Fearful of finding itself at a disadvantage, one challenger might decide to strike first, lest it lose the ability to retaliate. Moreover, when actions to defend look like plans to attack, stability can also be undermined by causing each side to conclude that war is inevitable.\footnote{Morgan, 2003p. 20.}

As with the nuclear domain, deterrence in space presents much of the same potential for instability, depending on how states decide to demonstrate the capability to deter. For examples, space deterrence will plausibly be relatively more unstable if states deploy large arsenals of ASAT systems; such systems may make war in space appear inevitable. If these missiles are postured in ways that makes them vulnerable to a preemptive attack, such a scenario could be even more unstable. Deployment of orbital ASAT weapons could also create “use or lose” incentives in a crisis to prevent an adversary from launching a first strike that would destroy or disable critical satellite systems. As in nuclear warfare, if a real or perceived fear that a first-strike advantage exists, as in the case of orbital ASAT systems, it may create pressures to reduce decision timelines, drive bias in analysis of indicators and warning, or limit opportunities for communication.\footnote{Mueller, 2013, p. 51.} Space assets are already viewed as essential enablers of a state’s warfighting capability, the destruction of which could shift the balance of forces and create an overwhelming military advantage.

Finally, a persistent debate in nuclear theory and practice that must be considered in a framework for deterrence in space is the idea of escalation. Specifically, such a framework must similarly grapple with whether escalation can be controlled. Although this debate persists in the nuclear community, partly because of the limited instances of nuclear escalation management, the scholarly literature provides many insights on the inherent challenges.\footnote{See Morgan et al., 2008, pp. 7–45, 68.} In nuclear deterrence theory, one side of the debate maintains that nuclear war can be kept limited, assured destruction is not a certainty, and nuclear war can ultimately be won.\footnote{Colin Gray, \textit{Modern Strategy}, New York: Oxford University Press, 1999, p. 314. See also Herman Kahn, \textit{Thinking About the Unthinkable}, New York: Horizon Press, 1962, pp. 194–219; and Paul H. Nitze, “Deterring Our Deterrent,” in Robert J. Art and Kenneth N. Waltz, eds., \textit{The Use of Force: Military Power and International Politics}, 3rd ed., Lanham, Md.: University Press of America, 1988, pp. 357–360.} The other side of the debate counters this position, noting that war planners have failed to demonstrate how such a war would be fought, how it would be terminated, and argues that control would likely be lost after exchanging tens of weapons.\footnote{Desmond Ball, “Counterforce Targeting: How New? How Viable?” \textit{Arms Control Today}, Vol. 11, No. 2, 1981, p. 8.}

A parallel conundrum can be seen in the effort to deter attacks in space. Two dimensions in particular must be considered. First, launching a limited strike against an adversary’s satellites is plausible, but it is difficult to ascertain whether a tit-for-tat retaliation would necessarily lead to
further escalation.\textsuperscript{54} Second, and perhaps containing a clearer path for escalation, the military capabilities enabled by each satellite vary; for instance, striking satellites that enable another state’s nuclear command and control capabilities (as opposed to weather satellites) seems inherently escalatory. All states capable of such attacks must perceive and understand this dynamic, though, for potential escalation dynamics to have a deterrent effect. Thus, one can see pathways to intentional, accidental, and inadvertent escalation in the space domain that will have to be managed for deterrence to hold.

As discussed in the first chapter, the Chinese military has articulated a concept of gradual escalation in space and other deterrence operations culminating in both reversible and destructive attacks on space systems. Chinese military theorists further argue that some space-based military weapons are akin to nuclear forces in their strategic deterrence effect, although the threshold for applying them is considerably lower than the threshold for employing nuclear weapons. These theorists caution that, although these “space weapons […] with strategic deterrent effect” should be used with discretion, their application can be decisive, and convincing demonstrations of their capability could achieve the effect of subduing an enemy without actual combat.\textsuperscript{55}

These similarities in mind, we must also be attentive to the significant differences between nuclear deterrence and deterrence of attacks on space assets. First, nuclear deterrence capabilities are highly visible, while some space deterrence capabilities, particularly cyber and electronic weapons, are not. Some analysts argue that the capability to attack another’s satellites will be in doubt—and thus lack deterrence leverage—until it is demonstrated in a crisis.\textsuperscript{56} Yet ASAT capabilities have been demonstrated in tests, and it is not clear that more capability is better; that is, it seems illogical that the United States or another state would need to have 1,054 ASAT tests for space deterrence to be visible and credible. Moreover, it is not clear that one must be able to retaliate \textit{in kind} for deterrence to prevail. If each side retains an ability to retaliate and inflict a prohibitively costly level of damage, or the ability to deny an adversary a \textit{fait accompli} even if its space assets are lost, then deterrence should be stable. Second, there are similarities and differences in the level and kind of destruction in the event of terrestrial nuclear strikes versus kinetic, debris-creating strikes on space assets. Both kinds of attacks would have catastrophic, indiscriminate environmental consequences. The costs of nuclear war, though, are usually framed in terms of massive loss of human life and lingering radioactive fallout, while war in space is framed in terms of long-term disruption of access to low-earth orbit with enormous economic and military consequences. To the degree that the latter is perceived to be qualitatively different from (and more manageable than) the former, deterrence may be undermined.\textsuperscript{57}

\textsuperscript{54} This path toward escalation is particularly uncertain because such a strike, by its nature, would not have occurred within the target state’s territorial boundaries and would also not lead to the loss of human life.

\textsuperscript{55} Jiang, 2013, pp. 57–58.

\textsuperscript{56} Krepon, 2013, p. 15; and Mueller, 2013, p. 55.

\textsuperscript{57} Mueller, 2013, pp. 54–55.
Cyber Deterrence

Leading experts on cyber warfare have illustrated that this type of warfare has distinct characteristics, including that the attacker’s identity can often be concealed, the defender can have difficulty predicting or understanding battle damage, and attacks dissipate quickly. As Martin Libicki notes, “cyberwar is nothing so much as the manipulation of ambiguity.”58 The challenges associated with deterring cyberattacks often parallel those cited for deterring attacks on space asset. These similarities include the challenge of attribution, credibility, proportionality of response, and the ability to control escalation.59

Both cyberattacks on information networks and attacks on space assets can be conducted by proxies or third parties using such techniques as spoofing or disruption of service that are not immediately conducive to attribution. Attribution is a necessary enabler of retaliation. Absent an ability to attribute and retaliate for an attack, deterrence threats are undermined because the cost of launching an attack would be essentially nonexistent. Yet if these types of attacks, whether in the cyber or space domain, represent holding a society hostage, the escalation of a crisis, or a prelude to war, it seems likely that demands (as well as reassurances to cease attacks if those demands are met) will accompany the attacks. It further seems likely that the country whose assets are under attack will know which state or states it is involved with in a crisis or conflict. It is possible that a third party could launch an attack to drive one side to escalate, so attribution is certainly important for identifying such malicious acts. Overall, although it may require time-consuming forensic work, the attribution challenge appears to be less intractable than some have previously argued.60

Second, as noted with respect to the nuclear domain, the credibility of one’s deterrence threats may also be questioned because of the “invisible” nature of cyber weapons and some space weapons. In addition, all-out cyber and space warfare have not occurred, which may lead to doubts about the effectiveness and the impact of such attacks on the outcome of the conflict. Both factors could potentially undermine deterrence threats.61 Yet the news is rife with reports of cyberattacks in the form of espionage, data theft, service disruptions, and spoofing. Threats of various forms of retaliation for cyberattacks, including economic sanctions and even military action, have proven ineffective in preventing attacks, so most cybersecurity efforts have focused on deterrence by denying benefit to attackers through improved defenses and resilience.

---

It also seems reasonable to conclude that states broadly understand the potential damage that an adversary could wreak in retaliation for a cyberattack. In his consideration of the application of deterrence theory to the cyber realm, Joseph Nye argues that denial plays a larger role in dealing with cyber threats from nonstate actors, but that punishment can be effective against both states and criminals. Nye concludes, “Preventing harm in cyberspace involves complex mechanisms such as threats of punishment, denial, entanglement, and norms.”

One could make the counterargument that, for cyber, once an otherwise invisible capability is made visible through a counterattack, the advantage is then lost by allowing an adversary to redress that vulnerability. But additional vulnerabilities will almost certainly exist. A state could judiciously launch attacks that do not reveal the most-damaging attack vectors available in its quiver against an adversary. Also, reports of cyberattacks against satellites are less prolific but still exist, thus demonstrating the capability, if not its full extent. Moreover, states possess visible space weapons in the form of ground-based missiles and jammers, as well as various orbital systems. For these reasons, although credibility may be a somewhat unique challenge in space and cyberspace as compared with the nuclear domain, these challenges appear to be surmountable.

The issues of proportional response and the ability to control escalation are related and thus discussed together. Unlike attacks in the nuclear domain, attacks in the cyber and space domains can often be reversible. Additionally, because such attacks can first materialize as limited or with unclear damage to critical civil and military systems—rather than manifesting with a visible human toll, as in conventional military or nuclear attacks—threats to retaliate for attacks in space and cyberspace may be viewed as disproportionate, escalatory, and incredible. Responding to such attacks may warrant a carefully calibrated retaliatory strike, and not necessarily one in kind. As in the cyber domain, calibrating retaliation in the space domain will likely be further complicated depending on the type of asset attacked. Punishment-based attacks may present a relatively greater challenge to retaliation. In these scenarios, to decrease the likelihood of escalation, it will be essential to communicate the damage done and how the retaliatory strike is proportionally tit-for-tat.

In her game theoretic modeling of space warfare, discussed in Chapter One, Bonnie Triezenberg found that tit-for-tat strikes when the opponent’s strategy was unclear were effective in maintaining deterrence and controlling escalation. With respect to denial-based attacks on military assets, the cyber and space domains likely face a similar challenge: Adversaries may

---

64 Glaser, 2011, p. 4.
65 Triezenberg, 2017, pp. 23–24, 64.
well perceive such attacks as a component of conventional war.\textsuperscript{66} A potential adversary may be particularly likely to take this view if the cyber or space assets under attack are understood to solely support one’s conventional capabilities. This factor suggests that perceptions of one’s overall military posture, and the connectivity between conventional and nuclear capabilities, will be crucial for space deterrence and limiting the potential for accidental and inadvertent escalation.\textsuperscript{67}

Finally, an important difference between nuclear deterrence and deterrence in the cyber and space domains is the standard of success. The goal of most nuclear weapon states has been total prevention of nuclear use, given the catastrophic consequences. As Nye notes, many aspects of cyber behavior are more analogous to other behaviors, such as crime, that governments strive to deter imperfectly.\textsuperscript{68} Given the complications noted earlier and the relatively low opportunity costs of launching cyberattacks on information systems, complete prevention of such attacks is not a realistic strategy. For some of the same reasons, governments lack the capabilities to deter completely all manner of reversible and destructive attacks on space systems. Yet it is plausible that states may seek the total prevention of debris-causing destructive attacks, similar to the total prevention in the nuclear context.\textsuperscript{69} This conclusion leads us to a consideration of what constitutes successful deterrence in the space domain.

\begin{thebibliography}{9}
\bibitem{66} Glaser, 2011, p. 5.
\bibitem{67} Glaser, 2011, p. 5.
\bibitem{68} Nye, 2016, p. 45.
\bibitem{69} Drawing out the analogy further, states may be unable to prevent nuclear strikes for demonstrative purposes. While the prevention of such strikes may be an objective, the prevention of a limited or large-scale nuclear strike is almost certainly the threshold requirement for nuclear deterrence success. In this context, successful deterrence in space may look relatively more like successful deterrence in a nuclear context.
\end{thebibliography}
Chapter 3. Defining Success in Space Deterrence

Classical Western deterrence literature suggests that a potential challenger’s motivations are the most important determining factor in deterrence success or failure.\textsuperscript{70} Because deterrence is a psychological undertaking, perceptions are paramount. Successful deterrence strategies seek to understand a potential challenger’s motivations, clearly communicate the actions one endeavors to deter, and demonstrate the capability and will to carry out those threats.\textsuperscript{71} As mentioned in the first chapter, the Chinese concept of \textit{weishe} (deterrence/coercion) focuses on influencing a potential aggressor’s perceptions and decision calculus and compelling it to adopt courses of action favorable to Chinese interests. Russia’s “reflexive control” strategy contains a similar approach.\textsuperscript{72}

In our earlier discussion of tailored deterrence, we noted that effectively using such a strategy requires detailed assessments of the leadership and society that another government seeks to influence, as well as integration of a broad variety of military, diplomatic, informational, and economic instruments. Robert Jervis’s examination of the role of psychology in deterrence of conventional conflict underscored that the decision-making calculus of governments satisfied with the status quo is more risk-averse than the calculus of those who are seeking to overturn it.\textsuperscript{73} The importance of understanding an adversary’s perception of the status quo is supported by behavioral economic analysis by Daniel Kahneman and Amos Tversky, which led to the development of the field of prospect theory.\textsuperscript{74} In her application of prospect theory in game theoretic analysis of space deterrence, Triezenberg concluded that a government’s perceptions about its country’s standing under the status quo have a larger impact on deterrence outcomes than any of the rational factors examined. These findings suggest that deterrence will be most effective if an adversary perceives that it has something to lose in any future conflict. This chapter explores these theories and concepts, specifically applied in the space domain, in more detail.

\textsuperscript{70} Morgan, 2003, p. 100.
What Is Space Deterrence?

The central goal of space deterrence is to prevent or limit nonkinetic and kinetic attacks against satellites and space support systems that would destroy those assets or significantly disrupt their operations. Nonkinetic attacks include electronic spoofing and jamming, cyberattacks, or the use of directed energy weapons (i.e., low-powered lasers, high-powered microwaves, and other radio frequency weapons) that can “dazzle” sensors or deny another government full use of its space assets. Kinetic attacks include physical attacks on ground sites; use of ground-based or air-launched ASAT missiles (direct ascent ASAT weapons); and co-orbital ASAT weapons with kinetic kill vehicles, lasers, chemical sprayers, and robotic mechanisms. Nuclear detonations in space could also be employed to degrade or destroy a space capability.\(^75\)

The objectives of overall deterrence and the objectives of space deterrence may differ. An example illustrates the distinction: Country A chooses to disrupt military satellite communications using nonkinetic means to prevent force direction commands from reaching the deployed fleet of Country B, thus blunting an attack. If Country B’s space deterrence succeeds, however, and Country A does not attack the satellite communication systems, Country A may pursue a kinetic attack on that fleet instead. In the above example, in deterring an attack in one domain, space, it led to an attack in a different domain to meet military or political objectives.\(^76\)

In that scenario, space deterrence was successful, but maritime deterrence was not—therefore, overall deterrence was unsuccessful—and a greater cost may have been paid in lives despite the successful space deterrence by Country B. While in this report, we focus the analysis on examining space deterrence independently of a broader deterrence context, we acknowledge that this is a simplification. Therefore, in application, it is important to consider the broader context in which space deterrence is sought.

---


\(^{76}\) Jeffrey Knopf takes a similar disaggregated approach when considering the need to deter asymmetric threats, such as terrorist organizations. See Jeffrey W. Knopf, “The Fourth Wave in Deterrence Research,” *Contemporary Security Policy*, Vol. 31, No. 1, 2010.
Measures of Success

The success of space deterrence is not binary. It should be measured along a spectrum that accounts for differing requirements for space services at various phases of a conflict and in light of how the conflict is unfolding in other domains. As escalation occurs or moderates, objectives of deterrence may thus shift from preventing attacks on space systems to preserving some future amount of space capability. This situation could emerge if, for example, concerns about generating debris that would pollute the space environment beyond the time horizon of the current conflict deterred the use of kinetic ASAT attacks. Yet, as will be discussed further, limitations to space deterrence exist, irrespective of what methods of deterrence are employed.\textsuperscript{77}

Broadly, perhaps the best measure of successful space deterrence is the extent to which a country’s deterrence actions influence an adversary’s decision to abstain from activities that diminish the deterring country’s space capabilities. However, the objective measurement of effective deterrence efforts depends on the requirements rooted in various dimensions. These dimensions may be time-based, event-driven, location-centric, dependent on multiple domains, connected to the space mission area, or dependent on weapon type. Michael Mazarr discusses similar deterrence trades (direct versus extended, general versus immediate, narrow versus broad), including limitations rooted in the “local balance of forces.”\textsuperscript{78} Combinations of these dimensions are also viable measures of space deterrence success.

*Time-Based*

One objective of space deterrence, and therefore a potential benchmark for success, may be to gain a sufficient time interval to build up reserves, activate backup resources, or maneuver to a position of advantage. By this standard, space deterrence could be a relatively fleeting requirement in practice but could require significant effort in the pre-hostility phase.

*Event-Driven*

Event-driven standards for space deterrence establish a specific event (without regard to the duration necessary to accomplish the event) as the anchor to which success is bound. Examples may include the deterrence of any degradation to position, navigation, and timing signals until after operations to seize the initiative (Phase 2 in U.S. joint military doctrine) are complete.

*Location-Centric*

Mindful that space mission architectures are composed of both terrestrial and exoatmospheric elements, this proposed category of space deterrence success is based on where an adversary


\textsuperscript{78} Mazarr, 2018, pp. 3–4.
attacks or withholds. *Location* is a catch-all here for several positional meanings. For example, space deterrence may be successful if there are no disabling attacks against space systems in low-earth orbit. More-demanding space deterrence objectives, though, may focus on successfully avoiding attacks against allied countries (to reinforce commitment to extended space deterrence) or against space assets in the homeland.

**Multiple Domains**

After hostilities are threatened (or openly begin) in another domain, space deterrence may manifest itself as a requirement whereby an attack on space capabilities must be avoided, even to the detriment of the other domain(s). Success for the space domain would be measured by the extent to which other domains bear the brunt of operations. The earlier example in which maritime and space platforms are both threatened is one in which cross-domain constraints may lead to measures of space deterrence success. Successful deterrence writ large would integrate acceptable outcomes across multiple domains.

**Space Mission Area**

Just as deterrence can be prioritized by domain, so too can space deterrence be prioritized by constituent mission area. Space mission areas have varying levels of importance to military operations and national strategic interests. A measure of successful deterrence could emerge from a prioritized list of missions or a subset of related missions, such as nuclear command and control or strategic missile warning.

**Weapon Type**

Looking to the lessons over the past six decades of nuclear arms control efforts designed to enhance deterrence, space deterrence could be enhanced by formal limitations on (or the elimination of) certain categories of counterspace weapons. Weapons perceived as having value against space systems include jammers, dazzlers, co-orbital rendezvous systems, kinetic direct-ascent interceptors, and exoatmospheric nuclear weapons. Establishing and abiding by limitations on such weapons or creating norms restricting their use could enhance the prospects for successful deterrence of certain counterspace actions.

**Impediments to Success**

Karl Mueller has elucidated why deterring an attack on various components of space systems is highly susceptible to failure in several contexts. These include when a state wants to convey a coercive signal with limited risks of escalation or collateral damage; when a state calculates that
there is a decisive advantage to be gained by counterspace actions; and, when there is an impetus to use or lose certain counterspace capabilities.\textsuperscript{79}

Two factors complicate the ability to deter hostile attacks on space assets. Reversible attacks are the most difficult to deter because adversaries plausibly assess that they face lower risks of a robust response or escalation—i.e., the consequences can be managed. Where it is difficult to present convincing proof of the source, and the attack can therefore be plausibly denied, it similarly presents a challenge to successfully deterring attacks in space. Patrick Morgan argues that “deterrence is not about keeping the challenger from getting what it wants; it is about constraining the means used.”\textsuperscript{80} Therefore, constraining the means used (for example, no destructive ASAT weapons) could be another criterion for successful deterrence.

**Selected National Approaches to Space Deterrence**

A review of several national approaches to space deterrence, and how these nations characterize success, provides useful insights in our effort to identify archetypes of space deterrence and a framework for identifying the strategies and postures of various countries or how they might be evolving. To gain the most analytic leverage in selecting which countries to consider, we kept roughly constant the existence of substantial space programs. For our purposes the variable of interest is variation in space deterrence approaches and postures. As such, the following five countries were selected for more detailed analysis: China and Russia, two U.S. competitors with established counterspace doctrines; France and Japan, two U.S. allies that are developing concepts of space deterrence; and India, a nonaligned nation that is in the early phases of developing its military space doctrine.

**China**

In Chapter One, we examined how the Chinese term *weishe*, generally translated as *deterrence*, which combines the Western concepts of deterrence and compellence, with a clear recognition of the psychological component. *Weishe* involves convincing an opponent both to refrain from a particular action and “to submit to the deterrer’s volition.”\textsuperscript{81} As a result, Chinese deterrence strategy is often considered closer to Schelling’s original concept of coercion and has some similarities with the Western concept of dissuasion.

Chinese military writings do not afford much attention to deterrence in the space domain per se; rather, they focus on the benefits of using space to pursue strategic deterrence and how actions targeting adversary space assets can deter hostile actions in another domain, as part of

\textsuperscript{79} Mueller, 2013, pp. 45–47.  
\textsuperscript{80} Morgan, 2003, p. 118.  
\textsuperscript{81} AMS, 2001.
China’s broader concept of integrated deterrence. The Chinese Academy of Military Science (AMS) authors of a core 2013 textbook for People’s Liberation Army space forces define the nature and goals of space deterrence accordingly:

“Space deterrence signifies having powerful space forces as backing and threatening to use or actually using limited space forces to awe and contain the opponent’s military activities. The goal of this activities pattern is to make a show of strength combining deterrence and combat and conduct activity to create a favorable posture, thus showing the real strength and resolve of the friendly space operations; generate doubt, fear, and wavering in the enemy; force him to abandon his operational intention; control the operational scale and intensity, plus the operational means; and thus achieve the goal of breaking the enemy’s resistance without fighting or with minimal fighting.”

The AMS strategists describe space deterrence (空间威慑 or 太空威慑) as a form of military deterrence akin to and working in tandem with nuclear and conventional deterrence to influence an adversary’s perceptions and actions. Space deterrence operations are not necessarily or exclusively designed to deter actions in the space domain. Because space deterrence is “strategic, convenient, and controllable,” the AMS strategists note that it has become the principal, more frequently used form of military deterrence. In line with broader Chinese thinking on deterrence actions, People’s Liberation Army training materials articulate the following concept of gradual escalation in space operations, culminating with attacks on adversary space systems:

- displays of space force capabilities in peacetime and the initial period of crisis using various media and diplomatic instruments
- realistic space military exercises, including simulations and ASAT tests, if space force displays prove insufficient and the crisis escalates
- space force deployment to improve preparations for conflict in space when the enemy has made clear moves toward combat
- overawing space attack, zhenshe daji, on an adversary to warn it that China has in place decisive preparations for war.

The AMS strategists describe two types of overawing attacks: (1) soft, including jamming, spoofing, and cyberattacks to disrupt reconnaissance, command and control, and

communications systems, and (2) hard, involving sudden, brief kinetic attacks of limited scope on sensitive enemy systems that convince enemy leaders to abjure hostile military operations and “accept terms under duress.”

Chinese military strategists present deterrence and actual combat as the two major modes of space operations that support the concept of active defense. Beijing’s active defense strategy is portrayed as defensive in nature, in that it seeks to gain the upper hand only after an enemy’s first strategic move toward conflict but then be capable of prevailing over the enemy, including through use of space offensive operations at the campaign and tactical levels. The Chinese military defines a space first strike in a unique way. They contend that, in advance of any military engagement, the United States (referred to as the “strong enemy”) will first conduct high-intensity space information reconnaissance operations that are decidedly different from such operations in peacetime. The nature of these operations constitutes a preemptive “first shot” in space combat operations, thus warranting a Chinese response. Chinese strategists also contend that, given changes in the nature of warfare, the “guiding ideology” of space operations is to launch space combat operations in advance of other military operations because space superiority is key to gaining information superiority, including in advance of modern “local” (limited) wars.

China’s general concept of deterrence and approach to the use of space for both deterrence and compellence are noticeably different from U.S. and other Western concepts of deterrence. China’s use of limited ASAT attacks in the service of deterrence would likely be interpreted by policymakers in the United States and other Western governments as initial escalatory acts to widen and intensify the conflict in ways designed to complicate crisis management. On the other hand, in the face of Chinese shock-and-awe attacks, efforts by the United States or other governments to de-escalate the crisis or identify off-ramps might be interpreted by Beijing as success of its space deterrence operations. This dynamic raises instability issues.

Russia

Russia’s 2014 Military Doctrine stipulates that space “supremacy” will be decisive in future conflicts as states seek to implement a modern system of warfare: high-precision, long-range strikes, and information dominance. Russian officials often highlight the alleged weaponization of space by the United States and have worked with China in the United Nations (UN)

---


87 Jiang, 2013, pp. 49–57.

88 Jiang, 2013, pp. 54–57.

Committee on Disarmament to promote the Treaty on the Prevention of the Placement of Weapons in Outer Space to prevent this development and what Moscow portrays as U.S. aspirations to dominate outer space.\textsuperscript{90}

Russian military planners view space as a warfighting domain and posit that U.S. reliance on space creates an Achilles’ heel that presents Moscow with a variety of opportunities to obtain its objectives and prevail in a conflict. Russia has developed a counterspace doctrine designed to deter aggression and, should deterrence fail, control escalation through “selective targeting of adversary space systems.”\textsuperscript{91} Russian doctrine envisions employing various ground-, air-, and space-based systems to disrupt or destroy adversary spacecraft and supporting infrastructure. Its so-called Strategic Operations to Destroy Critically Important Targets strategy is intended to employ dosed levels of damage to seize or retake the initiative and includes striking communication nodes and space surveillance segments.\textsuperscript{92} Russia’s direct-ascent ASAT missile attack against one of its own satellites on November 15, 2021, which created a large debris field, is suggestive of an offensive counterspace doctrine—or at least demonstrates that Russia could adopt such a doctrine. Given that this satellite was not at risk of tumbling out of orbit and causing terrestrial harm, this action further suggests that Russia has not accepted the norm that such ASAT attacks are destabilizing and undermine peaceful access to space for all governments and other users.\textsuperscript{93}

Russia’s concept of New Generation Warfare is a strategy of cross-domain coercion, integrating information warfare, the threat of nonnuclear precision strike, and limited nuclear strike to deter and compel adversaries.\textsuperscript{94} Although a focus of Russia’s military modernization effort has been to overcome its command-and-control deficiencies, Russian doctrine emphasizes not becoming overly reliant on space-based capabilities. Instead, Russian doctrine focuses on tactical-level ISR and command and control.\textsuperscript{95}


\textsuperscript{91} U.S. Defense Intelligence Agency, 2022, p. 22.

\textsuperscript{92} Dave Johnson, \textit{Russia’s Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds}, Livermore, Calif.: Lawrence Livermore National Laboratory, Center for Global Security Research, Livermore Papers on Global Security No. 3, February 2018. Other words that have been used to describe “dosed” escalation include deterrent, assigned, and unacceptable.


\textsuperscript{94} Adamsky, 2015, pp. 19–26.

\textsuperscript{95} U.S. Defense Intelligence Agency, 2022, p. 21.
Starting in the late 2010s, French defense planners have initiated efforts to protect France’s space-based C4ISR assets—which are critical to the operations of all its defense capabilities—from emerging threats. Until recently, French satellite threat assessments focused on ground-based risks, such as communications jamming, cyberattacks, the use of lasers to dazzle or damage satellite sensors, or missile interceptors. Growing concern about on-orbit threats, however, has prompted Paris to consider passive and active protection for its future satellites. In 2018, Paris accused Moscow of using a Russian satellite for on-orbit espionage, targeting a Franco-Italian military communications satellite.\textsuperscript{96}

The French government promulgated its first Defence Space Strategy in July 2019. A central goal of the strategy is to ensure France’s freedom of decision and action in space. Minister of Defense Florence Parly announced a new weapon program called Maîtrise de l’Espace (Space Control) to integrate improved space situational awareness (SSA) capabilities and active defense measures, including

- enhanced SSA systems to improve identification and characterization of hostile acts in space
- measures to improve the protection of national and key European space assets, such as cameras to provide warning of an approaching satellite that could represent a threat to enable defensive maneuvers and the placement of lasers on board major satellites and “patrol nano-satellites” for active defense that could dazzle hostile space systems.\textsuperscript{97}

France maintains that its space strategy is designed to enhance self-defense capabilities. The Ministry of Defense is also considering steps to ensure continuity of space services, including the development of nano-satellites and other capabilities that could rapidly provide ISR or communications if existing satellites were damaged or destroyed.\textsuperscript{98}

Maintaining freedom of access, upholding peaceful and responsible use, and acting in accordance with international law underpin the legal aspects of the space strategy. Paris remains committed to the Outer Space Treaty and to various international agreements designed to foster responsible behavior in space. The strategy calls for a clearer interpretation of the law of state responsibility regarding space activities. France asserts its right to be able to respond to activities that it considers hostile through countermeasures or active defense.

Japan

The Japanese government’s recognition of the importance of space to national self-defense grew incrementally over the past 20 years, consequent from the threats to its security posed by North Korea’s ballistic missile and nuclear weapon programs and growing Chinese military power, including counterspace capabilities.

Under the National Defense Program Guidelines for 2019 and Beyond, the Japanese Ministry of Defense is planning to build a “multi-domain defense force” able to deter and counter superior forces and sustain operations in all phases of conflict. Developing new capabilities in space, cyberspace, and the electromagnetic spectrum and integrating them with the traditional domains of land, sea, and air are given high priority.99 Japanese national space policy continues to shift from using space assets for nonmilitary purposes to enhancing capabilities that support terrestrial military operations and protect national security space assets.

The Japan Self-Defense Force has announced that, to “ensure superiority in use of space at all stages from peacetime to armed contingencies, the [Force] will also work to strengthen capabilities, including mission assurance capability and capability to disrupt opponent’s command, control, communications and information.”100 It is still unclear when and how the latter part of this policy will be implemented in the context of Japan’s self-defense guidelines.101 Japan has no declared offensive counterspace capabilities.102 In response to concerns about the ASAT, communications jamming, and other threats that various countries pose to Japan’s space systems, Japan’s defense ministry created a Space Operations Group, which will eventually include two SSA-focused space operations squadrons. The first squadron was stood up in May 2020, and a new space monitoring system is expected to begin operations in 2023.103

India

Indian leaders also appear to have a growing appreciation for the military importance of space and its role in deterrence across various domains. As one senior official said, “Space has

102 The Secure World Foundation’s 2022 report states, “While Japan does not have any acknowledged offensive counterspace capabilities, it is actively exploring whether to develop them. Japan does have a latent ASAT capability via its missile defense system but has never tested it in that capacity” (Weeden and Samson, 2022, p. xxii).
gained importance in the military domain. The best way to ensure security is to have deterrence.”104 Another senior space official linked India’s development of nonkinetic counterspace technologies with deterrence.105 The Indian government framed the March 2019 destructive ASAT test code-named Mission Shakti as being explicitly for deterrence: “The capability achieved through the anti-satellite missile test provides credible deterrence against threats to our growing space-based assets from long-range missiles, and proliferation in the types and numbers of missiles.”106 However, Prime Minister Narendra Modi and other officials also framed the 2019 ASAT test as a defensive technological experimentation to meet future challenges and counter threats from emerging technologies.107

The effect of the 2019 ASAT test was debated by Indian and foreign analysts. Some argued that the test was targeted solely at China and required generating debris to be a credible demonstration. However, other analysts doubt whether the ASAT test successfully restored India’s deterrence against China, arguing that it, at best, may deter Chinese kinetic ASAT attacks, which are of decreasing importance to Chinese counterspace operations, given the variety of other systems Beijing is developing.108 Indian scholars argue that the nature of modern warfare inevitably extends to space and that India must develop other counterspace capabilities (nonkinetic appears favored over kinetic) to pursue space deterrence, especially against China.109

Measuring Success and Comparative Strategies for Space Deterrence

The discussion of how to define success in the pursuit of space deterrence and the characterization of these various national perspectives on deterrence in the space domain, reveals several key points that inform our identification of archetypes of space deterrence, elaborated in Chapter Four.

Success in space deterrence—specifically, preventing or limiting nonkinetic and kinetic attacks against satellites and space support systems—may be measured along a spectrum instead

104 “Indian Space Wars: India’s DRDO Head Outlines Counterspace Capability Ambitions,” Space Watch Asia Pacific, April 2019.
of a binary manner. The objective measurements of effective space deterrence efforts may be time-based, event-driven, location-centric, dependent on multiple domains, connected to space mission area, or dependent on weapon type. The prospects for complete success in deterring hostile attacks on space assets, particularly reversible, nondestructive attacks, are limited. A space deterrence strategy focused on mitigating damage and preserving essential C4ISR capabilities through a mix of defensive and offensive counterspace actions, resilience measures, and reconstitution is most likely to be successful.

Our review of the variation in national approaches to space deterrence reveals several additional insights in developing the framework for archetypes of space deterrence. The Chinese and Russian concepts of space deterrence appear to reflect aggressive counterspace postures and doctrines designed to use the threat of disruption or destruction of critical space capabilities to intimidate the United States (or any other adversary) from initiating or prosecuting a conflict. Strategists in both countries assess that heavy U.S. reliance on space to support military operations creates asymmetric opportunities to disrupt space support and prevail in a conflict. The French and Japanese approaches to space deterrence, on the other hand, emphasize improved SSA and passive defenses, along with various resilience measures, to enhance mission assurance and thus deny potential adversaries’ success in counterspace attacks. However, French doctrine also calls for active defense measures to avoid or dazzle hostile space systems, and Japanese officials have discussed developing the capability to disrupt an opponent’s C4ISR capabilities. Indian thinking is still evolving, but the government cast its March 2019 destructive ASAT test as designed to bolster deterrence, suggesting that India is not content to rely only on resilience measures to maintain its space capabilities.
Chapter 4. Framework for Deterrence in Space

This chapter advances three archetypal strategies for space deterrence, integrating our earlier analysis of the foundational principles of deterrence, relevant lessons for space from the nuclear and cyber domains, criteria for success in deterring attacks on space assets, and selected national concepts of space deterrence. The archetypes provide a framework for assessing the deterrence strategy and goals of different countries in the conduct of their space operations and for illustrating how a nation can effectively deter attacks on its space assets.

Archetypes of Space Deterrence

Our analysis suggests three broad archetypes of space deterrence:

1. **Denial-dominant**: Deterrence that relies primarily on resilience, stealth capabilities, defensive measures, and redundancy to convince an adversary that it would be unable to achieve decisive advantage by attacking the target country’s space systems. This archetype may include some active defenses but limited capability to degrade the space systems of other countries. This approach also seeks to regulate the use of force in space through norms and sanctions for bad behavior. The French and Japanese strategies fall into this category.

2. **Mixed deterrence**: Deterrence pursued via a mix of resilience and defensive measures, combined with robust active defenses of space assets and more-substantial capabilities to degrade the space systems of other countries. This approach also sees merit in trying to regulate the use of force in space through norms and sanctions for bad behavior. These characteristics are reflected in the U.S. and Indian strategies.

3. **Offense-dominant**: Deterrence that includes elements of denial and resilience but relies more on punishment. This approach places emphasis on a wide variety of counterspace weapons capable of severely degrading the space systems of other countries, possibly combined with the threat of debilitating responses in other domains. This approach is designed to convince an adversary that it has much more to lose in attacking another country’s space systems, because any threat of or actual attack will result in robust counterspace actions. Norms are not a priority for states with this posture because they do not trust most other spacefaring nations to uphold them. Russia and China have adopted this approach.

None of the archetypes appears more predisposed to success or failure than the others. Each has its strengths, vulnerabilities, and required investments. Previous analysis and wargaming by Forrest Morgan and others at the RAND Corporation suggests that no single deterrence strategy, whether based on threats of punishment or on measures to deny benefits of an attack, would likely be completely credible and fully effective in deterring a capable adversary from attacking
an opponent’s critical space assets, particularly if a wider conflict appears inevitable. This suggests that an integrated approach to space deterrence—one that seeks to regulate the use of force and enhance stability through political agreements or international treaties on the norms of space behavior; ostracizes states that violate such accords; and allows states to retain some capacity to punish space aggressors in multiple domains and to develop measures to enhance the defenses, resilience, and redundancy of space systems—may have the greatest probability of success.

As discussed in Chapter One, deterrence is inherently psychological and linked to an adversary’s perceptions of the status quo and how its actions will sustain or improve circumstances to its benefit. The underlying informational needs—and how well each side is postured to meet these needs—will also influence a nation’s choice of deterrence methods. If leaders of one state are known to hold deeply seated beliefs about an adversary’s capabilities and willingness to use them, officials and analysts must treat this information as if it is true, even if it is not. Similarly, if those leaders assess that an adversary’s declared capabilities may not exist, denial-dominant deterrence may be seen as an acceptable policy. The elements of each archetype are described in Table 4.1.

Table 4.1. Elements of the Three Archetypes of Space Deterrence

<table>
<thead>
<tr>
<th>Element</th>
<th>Denial-Dominant</th>
<th>Mixed Deterrence</th>
<th>Offense-Dominant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctrine</td>
<td>Pursuit of assured access to space</td>
<td>Perpetuation of assured access to space</td>
<td>Dominance of space key to winning conflict</td>
</tr>
<tr>
<td></td>
<td>Emphasis on stability</td>
<td>Hedging on uncertainty</td>
<td>Emphasis on punishing attacks</td>
</tr>
<tr>
<td></td>
<td>Restrained counterspace messaging</td>
<td>Assertive counterspace messaging</td>
<td>Aggressive counterspace messaging</td>
</tr>
<tr>
<td></td>
<td>Promotion of responsible space behavior or code of conduct</td>
<td>More-explicit red lines</td>
<td>Distrust of norms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Promotion of responsible behavior or code of conduct</td>
<td>Clear red lines</td>
</tr>
<tr>
<td>Strategy</td>
<td>Emphasis on stealth, resilience, and defensive counterspace measures</td>
<td>Robust resilience and reconstitution measures</td>
<td>Space supremacy decisive in conflict</td>
</tr>
<tr>
<td></td>
<td>Partnership with allies and partners to enhance resilience and redundancy</td>
<td>Selective offensive counterspace to control escalation</td>
<td>Seizure of the initiative</td>
</tr>
<tr>
<td></td>
<td>Limited offensive counterspace capabilities held in reserve</td>
<td>Reservation of the right to disable hostile space actions</td>
<td>Escalation of counterspace attacks for cross-domain dissuasion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shock-and-awe attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Denial of adversary’s use of space (blockades)</td>
</tr>
<tr>
<td>Capabilities</td>
<td>Considerable ground and space SSA for attack warning</td>
<td>Enhanced ground and space SSA systems for attack warning and targeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passive and active defenses</td>
<td>Substantial passive and active defenses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyber defenses of ground stations and orbital systems</td>
<td>Defensive and offensive cyber capabilities versus ground stations and orbital systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limited offensive counterspace capabilities</td>
<td>Ground and orbital jammers,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passive defense maneuvers</td>
<td></td>
<td>Robust ground and space SSA systems for attack warning and targeting</td>
</tr>
<tr>
<td></td>
<td>Some reconstitution capabilities</td>
<td></td>
<td>Substantial cyber and electronic warfare counterspace assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Responsive battle management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C4ISR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Extensive ground and orbital jammers, lasers</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction of dependency on space support</td>
<td>Lasers, Some ground-based and orbital ASAT weapons, More-substantial reconstitution capabilities, Many ground-based and orbital ASAT weapons, Direct ascent ASAT weapon, Nuclear/nonspace, Rapid reconstitution capabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exercises/operations</td>
<td>Reflection of doctrine: stealth, maneuvers, passive and active defense, Exercises with allies and partners to demonstrate and test resilience, Restained ASAT testing, Stealth, maneuvers, passive and active defenses, Exercises with allies and partners to demonstrate and test resilience, More-visible ASAT operations and testing, Stealth, maneuvers, passive and active defenses, Exercises with allies and partners to demonstrate ASAT capabilities, Extensive open and covert ASAT operations and testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization/force management</td>
<td>Possible integrated space and cyber forces for defense, Improved cross-service and cross-domain C4, Fuller coordination of space and cyber forces, More-capable cross-service and cross-domain C4, Tightly integrated space and cyber forces, Robust cross-service and cross-domain C4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Elements For Space Deterrence Analysis

Deterrence analyses in general should consider the same building block elements, which will be present in each domain in differing mixes. Each of these elements should be considered, regardless of which element(s) are more predominant. The elements are:

- **stability**: the desire or intention to maintain strategic and crisis stability
- **credibility**: the degree to which an actor has the means to follow through on stated actions
- **escalation**: an increase in the severity of actions or rhetoric due to an adversary’s actions
- **signaling**: conveying a position or belief to an adversary
- **scope**: the span of affected weapons, defenses, and actors
- **willingness**: the level of stated or perceived intention to follow through on stated actions.

It is critical to consider these elements from both an adversary’s and allies’ perspective. When these elements are taken together, it may become clearer which model of deterrence is best suited for the circumstances. Table 4.2 summarizes each of these in the context of the three archetypes described earlier.
Table 4.2. Elements of Deterrence in the Space Domain, by Archetype

<table>
<thead>
<tr>
<th>Element</th>
<th>Denial-Dominant</th>
<th>Mixed Deterrence</th>
<th>Offense-Dominant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stability</td>
<td>Emphasis on first-strike stability New offensive capabilities viewed as destabilizing until defense measures are in place Preference for widely accepted norms Pursuit of only those counterspace capabilities that are perceived as capable of blunting an adversary attack or denying an adversary the use of threatening space assets</td>
<td>Potential pursuit of partnerships but a preference for a “first-among-equals” role Choice of the nature and timing of selective revelation of counterspace capabilities to have desired impacts on deterrence and crisis stability Support for norms Pursuit of advantages in multiple domains</td>
<td>Pursuit of first-mover advantage to unilaterally impose order Threatened by parity or near-parity Revelation of some counterspace capabilities, retaining others for surprise Pursuit of advantages in multiple domains</td>
</tr>
<tr>
<td>Credibility</td>
<td>Routine testing of backup and alternate capabilities Preference for cross-domain capabilities and solutions Judicious revelation of limited offensive capabilities</td>
<td>Demonstration of robust backup and alternate capabilities, including cross-domain capabilities Periodic demonstrations of offensive capabilities Sensitive to the appearance of fallibility or indecisiveness Frequent sharing of weapon test successes</td>
<td></td>
</tr>
<tr>
<td>Escalation</td>
<td>Risk-averse to avoid provoking attacks Willing to make some concessions to preserve the status quo Embrace of lateral escalation to increase stability</td>
<td>Participant in “gray zone aggression” as a precursor to counterspace attacks Response to ambiguity is to offer off-ramps to de-escalation and measured responses Potential embrace of a strategy of “escalate to de-escalate” Accepting of more risk through overlap (and interdependence of) cyber and nuclear warfare and activities in space Pursuit of decisive advantages politically and militarily</td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>Sharing of defensive test successes Advertisement of allied exercises Effective shaping of the adversary with consistent messaging postures</td>
<td>Demonstration of robust defenses and resilience Covert pursuit of some offensive weapons Vigilant intelligence for early warning Visible displays of offensive weapon testing Intelligence focused on adversary weaknesses</td>
<td></td>
</tr>
<tr>
<td>Scope and willingness</td>
<td>Touting of partnerships in all aspects of space efforts Receptive to space control agreements, even self-restraining Integration of domains to increase escalation potential and complicate adversary planning</td>
<td>Careful management of perceptions of national intent and will to enhance deterrence Integration of counterspace actions with conventional attack to increase chances of prevailing and reduce the costs</td>
<td>Large-scale maneuvers and exercises Establishment of “hand-tying” commitments for automaticity of response</td>
</tr>
</tbody>
</table>

Situational Considerations Affecting Outcomes

Consideration of the situational application of these approaches provides further insight when attempting to reconcile observed behavior into the deterrence archetypes described earlier. What follows are a series of vignettes to explore the benefits and risks of the denial-dominant and offense-dominant approaches (and, by extension, the mixed deterrence approach for border cases).
Denial-Dominant

Forest Morgan illustrated how a resilient, redundant, and integrated space architecture, in which adversaries see little advantage in attacking space capabilities, provides a strong foundation for effective deterrence by denial. To successfully embrace a denial-dominant deterrence posture, a country needs to have—or lead an adversary to perceive that it has—a very robust ability to neutralize attacks in many forms. This would mean absorbing an attack with a resilient architecture that continues to provide services unimpeded or that nullifies the attack. This posture could be achieved through highly effective space situational awareness capabilities, a mix of active and passive defenses, and cooperation with allies and partners in sharing services. Mission-assurance measures, such as stealth, evasive maneuvers, and capabilities for reconstitution of damaged or destroyed orbital and ground assets, could also raise the threshold for deterrence failure in the face of an adversary’s destructive counterspace attacks.

The messaging posture to support this approach would seek to ostracize the use of force in space, emphasize the importance of stability and maintaining access for all space-faring nations, and promote the development of norms of responsible behavior in space. The posture would also warrant considerable—albeit not necessarily complete—transparency about the country’s space architecture and demonstration of its redundant capabilities in exercises and testing of new systems. Creating the impression that some undisclosed capabilities are already parked in orbit or available on the ground for rapid deployment might also strengthen the credibility of this approach. A country pursuing this strategy might want to maintain some offensive counterspace capabilities to be used in a tit-for-tat fashion to threaten an adversary’s space or counterspace assets, but with the goal of providing off-ramps for de-escalation.

This approach is most promising in two cases, which are not mutually exclusive. The first case is one in which the deterring nation is highly capable, as described earlier. The second case is one in which the country to be deterred is not heavily reliant on space. This does not strengthen the denial-dominant effort per se, but it makes this approach more favorable because the offense-dominant model is less potent against an adversary that is only marginally dependent on space.

Offense-Dominant

Offense-dominant deterrence is a potentially riskier, more costly, and more demanding approach with greater potential for escalation between hostile countries. To the extent that deterrence holds, the archetype is not necessarily more dangerous than the other options. However, if deterrence fails and the would-be deterred country initiates hostile action, the punitive actions by the target country may accelerate the pace of conflict. If, on the other hand, the threatened punishment is perceived as beyond the threshold of endurance, this approach

would succeed. The potential for catastrophe is high if this method fails, particularly if the state pursuing it is highly dependent on space support.

This approach would support a strategy of achieving dominance and control in space by initiating preemptive counterspace actions against an adversary before it strikes. It would require substantial ground and orbital defensive and offensive counterspace systems, many—but not necessary most—of which have been revealed to the international community and regularly tested in exercises. This strategy might conceal or hold in reserve certain high-end counterspace capabilities for shock-and-awe attacks, as articulated in Chinese doctrine, that are designed to terminate conflict, at least in space, on the adversary’s terms. The approach would need to be supported by robust SSA, attack warning, and space battle management command and control capabilities.

The messaging posture to support this approach would be aggressive, avowing a willingness to respond forcefully and in a robust manner in space and other domains to any threats to critical national space capabilities. Somewhat like extended deterrence, this approach might involve explicit or implicit red lines and a hand-tying commitment—that is, a demonstration of a capacity for automaticity of response to an attack or the threat of attack, which would further complicate escalation management.112 Such a strategy, particularly the revelation of additional counterspace capabilities in the midst of a crisis, could lead the country it was seeking to deter to conclude that it needed to attack the adversary’s space and counterspace capabilities as much as possible, to avoid a decisive defeat. Norms are not a priority for states with this posture because they do not trust most other spacefaring nations to uphold them.

This approach could be effective in deterring a country that is heavily reliant on space for the conduct of its military operations and that either has a limited number of assets or has a large catalog of space assets but has undertaken limited resilience and mission-assurance measures.

**Mixed Deterrence**

The mixed approach would support a hedging strategy, seeking to leverage the strengths and opportunities of deterrence by denial and deterrence by punishment while minimizing the downside vulnerabilities and risks of each. This archetype would rely heavily on passive and active defenses, resilience, redundancy, and some reconstitution capabilities to convince an adversary that an attack on the target country’s space systems would not be effective. This approach would also require investing heavily in SSA and attack warning and characterization systems in a more substantial suite of offensive counterspace capabilities than is required in the denial-dominant approach. This approach also sees merit in trying to regulate the use of force in space through norms and sanctions for bad behavior. Countries using this archetype would pursue a more assertive messaging strategy, including a declaratory policy with more-explicit red

---

112 See Mazarr, 2018, p. 3.
lines, more-frequent and more-visible counterspace exercises with allies and partners, and higher-profile tests of new counterspace systems.

One downside risk could be that this approach sends mixed messages to an adversary and results in greater risks of escalation or even preemption.

**Possible Contribution of Norms**

Although the 1967 Outer Space Treaty prohibits state parties from placing weapons of mass destruction in orbit around the earth, installing these weapons in outer space, or installing them on celestial bodies, the agreement leaves significant gaps, including the use of conventional weapons against space assets. Article IX of the treaty does stipulate that all state parties “should conduct all their activities in outer space . . . with due regard to the corresponding interests of all other States Parties to the Treaty.” Building on this principle, and in an effort to fill this gap, there has been considerable effort in UN committees and other international fora over the past few decades to develop non–legally binding norms that would bolster responsible space behavior—for example, a norm that states should eschew destructive ASAT tests and other activities that would add to debris in space. Other norms that have been under discussion in the international community include (1) guidelines (such as a set stand-off distance or acceptable rates of closure) in the conduct of rendezvous and proximity operations (RPOs) against another state’s satellites without permission and (2) norms for on-orbit servicing of satellites, which could be used not only to repair but also to damage or destroy another state’s satellite.

The U.S. government has signaled over the past decade its interest in international discussions of non–legally binding norms of space behavior and conducted a round of talks with senior Russian officials on this subject in July 2020. The United States, along with other governments and nongovernmental organizations, contributed ideas in support of a UK initiative to undertake UN General Assembly dialogue on major space threats, seeking to build awareness

---

113 United Nations General Assembly, “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,” New York, January 27, 1967. Although Article IX has been ignored by several governments in practice, it is seen by many legal experts as a fundamental norm that proscribes actions in space that would compromise the space interests of other treaty signatories; examples of such actions include debris-creating ASAT tests that could imperil safe operations and active interference in the functioning of another state’s space systems through jamming, dazzling, or disrupting control links.

114 For an insightful review of past and ongoing efforts to develop space norms and arms control measures, see Paul Meyer, “Arms Control in Outer Space: Mission Impossible or Unrealized Potential?,” Calgary and Ottawa: Canadian Global Affairs Institute, October 2020.

and consensus on responsible space behavior and to catalyze further discussion on norms. These ideas were collected in a September 2021 report by the UN Secretary General and form a basis for ongoing discussions on responsible space behavior in various international fora. Further energizing the development of norms of space behavior, U.S. Vice President Kamala Harris announced in April 2022 that the United States would refrain from conducting destructive, direct-ascent anti-satellite missile testing and seeks to establish this as a new international norm for responsible behavior in space. Although imperfect and not enforceable, non–legally binding norms of space behavior could help build confidence among space-faring nations and enhance stability and deterrence by creating rules of the road and thresholds that would be clear warnings of hostile intent.

Impact of Messaging and the Revelation of Capabilities

Space-related strategic messaging can have significant impacts on the effectiveness of each of the three archetypes in shaping adversary behavior and on deterrence stability, crisis stability, and de-escalation. Messaging involves the interaction of a variety of statements and actions by a country, whether intentional or inadvertent, that influence the perceptions of its allies and adversaries, as well as domestic audiences. Messages are conveyed through documents on national space strategy, formal policy pronouncements, informal comments by political and military leaders, military doctrine, and publications by officially linked sources (such as professional military education intuitions). Such messages are actualized and amplified by on-orbit operations, space force training, national and multilateral military space exercises, tests of new space systems, and acquisition of space capabilities. A country’s space-related strategic messaging can help enhance overall stability, dissuade adversaries from initiating a military space competition, assure allies that the country has measures in place to protect mutual interests, and deter an adversary from initiating an attack.

How these messages are conveyed, based on various attributes, which can be calibrated, will affect their impact on various audiences. These attributes include the content of a document or policy pronouncement, the tone (restrained or assertive), the classification, and who is delivering the message—a head of state, a lesser national leader, or a military commander. The attributes of messaging actions that can influence their impact include their timing (in peacetime or crisis),

116 For an insightful nongovernmental contribution, see Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O’Connor, Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity, Santa Monica, Calif.: RAND Corporation, PE-A887-2, 2021.
their transparency (overt or concealed), and whether they are routine or unprecedented. Some examples of how messaging can bolster the approaches to deterrence are illustrative:

- **Denial-dominant**: Country C’s national space strategy proclaims a commitment to stability in space and assured access to all peaceful, space-faring nations, and national leaders issue statements that emphasize adherence to the principles of the Outer Space Treaty and urge development of norms for responsible space behavior. The country’s space strategy is transparent and emphasizes resilience and defensive measures, which are also reflected in the testing and acquisition of space assets, military doctrine, training, and exercises with allies and partners. In the context of a crisis with Country D, which is threatening or has initiated counterspace strikes, Country C seeks paths to de-escalation, undertakes defensive measures to protect its space assets, and limits any counterspace actions to proportionate tit-for-tat strikes on Country D.

- **Offense-dominant**: Country E’s national space strategy emphasizes its intent to maintain superiority in space and dominance in all phases of conflict. Its declaratory policy sets out clear red lines and a willingness to engage in an escalating series of counterspace actions to maintain dominance over any aggressor. Before a crisis, it has previously developed, in a visible manner, a variety of counterspace weapons capable of severely degrading the space systems of other countries, and it has regularly tested these weapons in military exercises, possibly combined with simulated cyber and kinetic actions designed to disrupt the space operations of other countries. The country might also reveal new counterspace capabilities in a crisis to achieve surprise, with the goal of coercing adversary Country F to cease its actions in space or in a terrestrial conflict.

Consistent messaging across the various levers of national action is critical and can be effective in shaping adversary perceptions of national intent and will and may also enhance deterrence. Dissonance in messaging can send conflicting signals to both adversaries and allies and lead to unintended consequences, particularly in a crisis. Finally, another factor influencing the effectiveness of space messaging in supporting deterrence is the feedback loop. The messaging state needs a capacity to assess whether intended messages have been received by various audiences, whether target states have the technical capability to observe related space actions, and how the target state is likely to react.

**Cross-Domain Considerations**

In closing, we offer some brief observations on cross-domain influences on space deterrence. Space deterrence is not a separate challenge and cannot be considered in isolation. Leaders of the major space-faring nations recognize that counterspace actions in the context of a conventional conflict against an adversary that is highly dependent on space for conducting its terrestrial military operations could increase the chances of prevailing and reduce the costs suffered in the course of the conflict. We noted earlier that the effectiveness of a state’s conventional deterrence capabilities also affects an adversary’s calculus in space, and cyberattacks provide a low cost, potentially effective way to disrupt and possibly damage an adversary’s ground-based and orbital space systems. Although the United States and other major governments have declared that
attacks on critical components of their space architecture would be seen as highly escalatory and would be met with a harsh response in various domains, Chinese writings have taken the perspective that attacks on enemy space systems are unexceptional, readily controlled, and could be used to avoid or terminate a conventional conflict. Finally, the overlap between nuclear warfare and activities in space—including the use of satellites for nuclear indications and warning, command and control, targeting, and post-strike damage assessments—underscores the interdependence of these two domains and the significant potential for deterrence failure and escalation.

The three archetypes of space deterrence strategies presented in this paper advance the conversation about how to pursue deterrence in the space domain. This initial effort to advance the state of the art in the field should be built on in future analysis that incorporates these cross-domain influences and interdependencies.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMS</td>
<td>Academy of Military Science</td>
</tr>
<tr>
<td>ASAT</td>
<td>anti-satellite</td>
</tr>
<tr>
<td>C4</td>
<td>command, control, communications, and computers</td>
</tr>
<tr>
<td>C4ISR</td>
<td>command, control, communications, computers, intelligence, surveillance, and reconnaissance</td>
</tr>
<tr>
<td>ISR</td>
<td>intelligence, surveillance, and reconnaissance</td>
</tr>
<tr>
<td>NPR</td>
<td>Nuclear Posture Review</td>
</tr>
<tr>
<td>SSA</td>
<td>space situational awareness</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>


AMS—See Academy of Military Science.


https://www.rand.org/t/RR1366


https://www.rand.org/pubs/working_papers/WR1027.html


“India Says Anti-Satellite Missile Test Aimed to Deter Threats to Its ‘Space Assets,’” Reuters, March 27, 2019.

“Indian Space Wars: India’s DRDO Head Outlines Counterspace Capability Ambitions,” *Space Watch Asia Pacific*, April 2019.


Johnson, Dave, Russia’s Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds, Livermore, Calif.: Lawrence Livermore National Laboratory, Center for Global Security Research, Livermore Papers on Global Security No. 3, February 2018.

Kahn, Herman, Thinking About the Unthinkable, New York: Horizon Press, 1962.


Krepon, Michael, and Julia Thompson, eds., Anti-Satellite Weapons, Deterrence and Sino-American Space Relations, Monterey, Calif.: Naval Postgraduate School, Center on Contemporary Conflict, 2013.


