REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03/28/2018	Research	

4. TITLE AND SUBTITLE
Celestial Deterrence: Deterring Aggression in the Global Commons of Space

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Eric J. Zarybnisky, Lt Col, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval War
College 686
Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited Ref: DODD 5230.24

13. SUPPLEMENTARY NOTES
A paper submitted to the Naval War College in partial satisfaction of the requirements of the NSA Department. The contents of this paper reflect the author's personal views and are not endorsed by the USNWC nor the military departments.

14. ABSTRACT
Preventing war in space is of the utmost importance because of the lasting effects such a war would have. Deterrence by denial is difficult for the four types of attacks against space assets: kinetic, non-kinetic physical, electromagnetic, and cyber. However, deterrence by punishment, specifically through horizontal escalation, is viable for kinetic attacks. International norms and a deterrence policy for kinetic attacks need to be developed. Additional effort is necessary to mature attribution and defense capabilities for the other types of attack and, possibly, to extend the theory and practice of deterrence to these types of attacks.

15. SUBJECT TERMS
Space, Deterrence, Kinetic Attack, Horizontal Escalation, International Norms

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Eric Jack Zarybnisky
UNCLASS	UNCLASS	UNCLASS	UU	18	19b. TELEPHONE NUMBER *(Include area code)* 719-964-7225

Celestial Deterrence: Deterring Aggression in the Global Commons of Space

Eric J. Zarybnisky

INTRODUCTION

General John Hyten, the commander of United States Strategic Command, stated that the United States needs to deter aggression in space due to the impacts such actions would have on the use of space for global communication, navigation and timing, and intelligence collection.[1] A collision between two low Earth orbit satellites in 2009 resulted in more than 2,000 pieces of orbital debris[2] all moving 9 times faster than a bullet[3] that will remain in orbit for decades.[4] This collision, and the resulting debris, demonstrate the magnitude of harm that could come from war in space. Prevention is of the utmost importance because of the lasting effects of a space war. While the immediate loss of life from a space war would pale in comparison to nuclear war, longer-term impacts would be catastrophic across a range of capabilities. In the case of geosynchronous orbit, some of the most valuable real estate in space, orbital debris could forever endanger everything including space-based satellite television, weather reporting, and missile warning.[5]

Unlike nuclear deterrence during the Cold War, deterring aggression in space does not have a fundamental philosophy such as Mutually Assured Destruction, which dictated a specific response to a nuclear attack. Reliance on satellites is neither equal among countries nor static over time. As more countries rely on space assets, policymakers need to understand the impact on deterrence, from both kinetic and non-kinetic engagements, to maintain the utility of the space environment. This paper argues that traditional deterrence theory is effective for kinetic space attacks but not for other types of attacks, namely non-kinetic physical, electromagnetic, and cyber. Underlying this argument is the fact that kinetic attacks can be readily attributed and a small number of countries have kinetic attack capability allowing for credible deterrence, which includes communication of the deterrent threat, without significant risk for miscalculation

between countries. Traditional deterrence theory is not effective for other types of attacks including non-kinetic physical attacks (e.g., lasers or high-power microwaves), electromagnetic attacks (e.g., jamming) and cyber attacks, due to the challenges of attribution. Deterring kinetic aggression in space requires policymakers to develop a credible deterrent through exercises, budgetary authority, new international norms, and mechanisms to prevent inadvertent escalation.

PREVENTING AGGRESSION IN SPACE

While deterrence and the Cold War are strongly linked in the public's mind through the nuclear standoff between the United States and the Soviet Union, the fundamentals of deterrence date back millennia and deterrence remains relevant. Thucydides alludes to the concept of deterrence in his telling of the Peloponnesian War when he describes rivals seeking advantages, such as recruiting allies, to dissuade an adversary from starting or expanding a conflict.[6] Aggression in space was successfully avoided during the Cold War because both sides viewed an attack on military satellites as highly escalatory, and such an action would likely result in general nuclear war.[7] In today's more nuanced world, attacking satellites, including military satellites, does not necessarily result in nuclear war. For instance, foreign countries have used high-powered lasers against American intelligence-gathering satellites[8] and the United States has been reluctant to respond, let alone retaliate with nuclear weapons. This shift in policy is a result of the broader use of gray zone operations, to which countries struggle to respond while limiting escalation. Beginning with the fundamentals of deterrence illuminates how it applies to prevention of aggression in space.

Deterrence requires that one group persuade an adversary that the cost of an action outweighs the perceived benefit.[9] Examining this definition highlights two main ways aggression in space can be deterred: by increasing the cost of an adversary's action or by reducing the

perceived benefit.[10] A country wishing to prevent aggression could choose to use one or both tactics. However, the growing reliance on space assets diminishes the second possibility since reducing the perceived benefit of an attack in space would require a capability, either space- or terrestrial-based, to replace a damaged or destroyed satellite. Even if the expense of additional satellites could be reduced through disaggregation or larger block purchases, an adversary that can attack one satellite would likely have the capability to attack multiple satellites. Terrestrial options are problematic since replication of satellite functionality, such as intelligence collection over denied territory, is difficult to accomplish in other domains.

Since reducing the perceived benefit of an attack is ineffective, increasing an adversary's cost must be the focus of a space deterrence policy. This increase can be accomplished through either denial, which seeks to increase the cost incurred before taking action by making an attack more difficult, or punishment, which seeks to increase the cost incurred after taking action.[11] The space domain presents challenges for deterrence through denial. Unlike ground forces, which can be protected from an enemy by fortifications, thus requiring an overwhelming force to assure victory, space does not offer such an advantage. Satellites are less defensible than most terrestrial assets because they "…move in predictable paths devoid of geographical cover.."[12] making them "…vulnerable to attack and difficult to defend."[13] Accordingly, a deterrence by denial strategy has little to offer for space because of this difficulty of defense.[14]

Preventing aggression in space needs to rely on deterrence by punishment. This strategy requires capability, resolve, and a punishment cost,[15] all of which need to be understood by an adversary. Most countries that rely on space have the demonstrated capability to inflict punishment on an adversary. These capabilities include conventional military forces, anti-satellite weapons, economic sanctions, and, possibly, nuclear weapons. Combining capability

with resolve poses two issues: the credibility of an in-kind response and the difficulty of attribution.

First, if a country relies on space for vital functions, how likely is that country to retaliate for an attack in space with another attack in space? The United States, Russia, and China have all demonstrated anti-satellite capabilities. Most recently, the Chinese tested an anti-satellite missile that destroyed a Chinese satellite in low Earth orbit, causing an estimated 3,000 pieces of orbital debris.[16] These pieces of debris will remain in orbit for years to come, affecting other low-Earth-orbiting satellites and space launches that must transit through the debris. An attack on a satellite in geostationary orbit would have longer-term, and higher impact, consequences. With this in mind, a country that views space as a vital national interest is unlikely to respond in kind to a satellite attack due to the debris risk to its use of space. While the Chinese example above shows that this is not an absolute deterrent, the punishment mechanism will likely occur in a different domain.

Attribution is the second issue arising at the intersection of capability and resolve; the threat of punishment is only credible if an adversary can be linked to the attack. Understanding attribution for a space attack requires consideration of the four different kinds of attacks: kinetic, physical attack via non-kinetic means, electromagnetic, or cyber.[*][17] While each of these attacks may result in the loss of a satellite, subsequent effects may differ. Additionally, technology used to attribute the source of an attack varies widely between these methods. A kinetic attack, such as an anti-satellite missile, is "…usually attributable…and the risk of collateral damage is high."[18]

[*] A kinetic attack seeks to irreversibly damage a satellite by hitting it with one or more objects. A physical attack via non-kinetic means seeks to irreversibly damage a satellite without contact, namely through directed energy (e.g., lasers or high-powered microwaves) or an electromagnetic pulse. An electromagnetic attack targets the communication links of a satellite through radio frequency interference and the effects are typically reversible. A cyber attack targets the computer systems and/or information on a satellite resulting in either reversible or irreversible effects.

Such an attack could even result in a loss of space as an operational domain for a century or more.[19] In fact, scholars liken the indirect effects of a kinetic attack in space to the use of biological weapons with incalculable long-term impacts; this uncertainty induces a level of self-deterrence upon nations who currently or seek to use space.[20] This self-imposed deterrence reinforces the idea that a country dependent upon space will not retaliate in kind to a kinetic attack in space.

In contrast to a kinetic attack, the other three types of attacks, non-kinetic physical, electromagnetic, and cyber, are all challenging to attribute.[21] For these types of attacks, obtaining information and determining the cause of a satellite malfunction requires days or weeks of investigation and analysis.[22] Investigating a satellite malfunction has been described as "…long-distance detective work."[23] For instance, when an Air Force strategic missile warning satellite failed in 2008, the investigation lasted over four months.[24] Since understanding the cause of a satellite failure is a precursor to attributing such an attack, such a delay drastically reduces the effectiveness of any deterrent. State and non-state actors understand the attribution problems that result from these types of attacks. They can exploit this fact, along with the possibility of reversibility, to degrade the effectiveness of a satellite while not crossing a perceived threshold that would invoke a response. A space wargame highlighted this phenomenon in which participants viewed kinetic attacks as "…more escalatory than even a non-reversible, non-kinetic attack."[25] With this in mind, participants in the war game turned to cyber attacks as the primary means of degrading space-based capabilities.[26] Since traditional deterrence theory is not effective for non-kinetic physical, electromagnetic, and cyber attacks, they must be addressed in another manner, possibly a new deterrence theory, an increase in satellite defense, or through dissuasion.

In light of these issues, preventing aggression in space is limited to deterrence of attributable attacks, namely a kinetic attack, coupled with a credible punishment. Since retaliation in space is not a viable strategy for countries with a strong reliance on space, horizontal escalation is the only credible way to deter adversaries from attacking space assets. Horizontal responses to aggression in space may include non-space-based military assets, economic sanctions, diplomatic pressure, and others.[27] Horizontal escalation, with its implied shift in domain,[28] is part of the current space deterrence dialog. General Hyten stated that attacks in space might not yield an in-kind response but rather a terrestrial one.[29] Beyond public statements, horizontal escalation has arisen in space wargames in which participants demonstrated a propensity to escalate horizontally, even to the point of kinetic attacks on terrestrial targets.[30]

Choosing how to escalate horizontally requires an understanding of what an adversary values, driving the decision for which targets to hold at risk. Unlike Mutually Assured Destruction, which directed a specific response to a nuclear attack, namely retaliation with nuclear weapons, there is no set response to a kinetic space attack. For example, the destruction of an aging Global Positioning System satellite should result in a different response than the destruction of a newly-launched, one-of-a-kind, intelligence satellite. To address these differences, flexible response policies are needed. Such policies give decision makers multiple options to choose from when responding to an adversary's actions.[31] These options need to consider the identity of the adversary.

Given the small number of countries that possess kinetic anti-satellite weapons, responses can be developed and tailored to possible attack scenarios by each adversary. Since deterrence is dependent on an adversary comprehending the capability, believing the resolve, and

understanding the costs, communication is essential. This communication is possible among a small number of countries with defined command and control structures. However, it is not just the opinion of these countries that influence the effectiveness of the deterrent.

Views of other countries, inter-governmental organizations, and non-state actors are influential and affect the perceived resolve of a retaliatory threat. Under Article III of the Outer Space Treaty, through its extension of international law and the United Nations' charter to space, self-defense in space is a legitimate response, including pre-emptive self-defense.[32] If a satellite is attacked, a country could invoke Article 51 of the United Nations' charter and respond within the bounds of distinction and proportionality. Accordingly, deterrence by punishment is valid under international law, thus reinforcing the perceived resolve of a country that employs this deterrent policy. In summary, the threat of punishment can be used to deter a kinetic attack in space, but the lack of attribution prevents the threat of punishment from being an effective deterrent against non-kinetic physical, electromagnetic, or cyber attacks in space.

NORMS, TARGETS, AND INADVERTENT ESCALATION

While nuclear deterrence played a pivotal role in restraining aggression during the Cold War, the modern space era is more complex and the fundamental objectives of nuclear deterrence and deterrence in space are different. Cold War nuclear deterrence sought to have no nuclear violence,[33] a standard well above what we can expect to achieve in space since numerous countries have already demonstrated a willingness to use both kinetic and non-kinetic weapons in space. Countries have not developed updated behavioral norms in space similar to the protocols established between the United States and the Soviet Union during the Cold War. In fact, space has been called "the Wild West."[34] Examples of norms that need to be codified, which mirror the American and Russian agreement to prevent incidents on the high seas, include

exclusion zones around satellites, deconfliction protocols for orbits, and agreements on acceptable space exercises. This lack of norms seriously diminishes the effectiveness of deterrence in preventing aggression, even among a small number of countries. Without norms, the line between behavior that will invoke a response, and behavior that will not, is not clear, making retaliatory threats less credible.

If the problem of attribution can be solved, deterring aggression still requires an appropriate response against a target that the adversary values and understands is at risk. For instance, what is the appropriate target to hold at risk to deter aggression against a communications satellite in geostationary orbit? A tit-for-tat strategy would suggest an adversary's comparable communication satellite, the ground station for such a satellite, or the command and control nodes that prosecuted the attack. Attacking a satellite is not an attractive option for a country that relies on satellites due to the potential for debris and future collisions, reducing the credibility of such a threat. Horizontal escalation, such as the two terrestrial options, requires finding such sites and developing an in-depth understanding of how an adversary values those targets, including other missions accomplished at those sites. A target needs to have sufficient value to affect the adversary's cost-benefit calculation but not so high as to provoke a preemptive response[35] or call into question the resolve to attack the target. Different methods of attack further complicate this issue. What results is an almost byzantine construct in which deterring aggression against a satellite will depend upon, at a minimum, the satellite's function and orbital regime, the method of attack, and the adversary's valuation of potential targets, which may change over time or as tensions rise. Even if the deterring state fully understands this construct, it must be unambiguously communicated to, and understood by, its adversaries. In light of these complications, military threats to deter aggression in space during peacetime are

likely not credible and, during wartime, an adversary will likely view the benefit of an attack is space outweighing the costs.[36]

A further complication for policymakers is understanding how adversary decision makers will respond to unforeseen circumstances. Any nation that uses deterrence by punishment to prevent aggression in space must face the reality that its adversaries will likely follow suit. If a natural event, such as a solar flare, causes satellites of multiple nations to become unresponsive, how will other nations respond? A country with sufficient space situational awareness capability could determine the cause of an issue and respond appropriately. However, this may not be the case for a country with lower space situational awareness proficiency. During a space war game, an Air Force official said that all possible responses were on the table when situational awareness was lost.[37] However, even with sound decision making and command-and-control processes, the uncertainty associated with space makes inadvertent escalation more likely.

While the challenges of target selection and possibility of inadvertent escalation are serious considerations, horizontal escalation remains a valid option for deterring a kinetic attack in space. Due to the small number of countries that can prosecute such an attack, coordination mechanisms can be established to lessen the possibility of inadvertent escalation. These mechanisms could mirror the framework built to lessen the possibility of inadvertent nuclear escalation between the United States and the Soviet Union. Similar logic applies to the challenge of target selection. Since the countries that possess kinetic-strike capabilities are world powers, each has an established understanding of the target valuation scheme of the others. This understanding, similar to the coordination framework, has its roots in the nuclear strike capabilities of these countries. The World Trade Organization illustrates another paradigm that could be used to address the coordination and target selection problems. Under this concept a set

of rules would be defined and if a country violates one of the rules, the victim of the transgression can retaliate using one or more prescribed methods.

CONCLUSION

Preventing aggression in space is in the best interest of many countries due to the growing dependence on satellites. However, the problem of attribution is a driving concern that limits the applicability of deterrence to kinetic attacks. The small number of countries that possess kinetic-strike capability enables the concept of horizontal escalation while addressing the concern for inadvertent escalation through frameworks similar to those established for nuclear deterrence. This logic does not extend to non-kinetic attacks.

With the rapid growth of technology since the end of the Cold War, transnational terrorists and other non-state actors, along with rogue states, now have access to advanced space capabilities, namely non-kinetic physical, electromagnetic, and cyber attacks, formerly available only to advanced countries.[38] Expansion of these three types of threats makes deterrence less stable.[39] Moreover, non-kinetic physical, electromagnetic, and cyber attacks are harder to deter due to the difficulty in determining the cause of a satellite failure and then determining who perpetrated the attack. Unlike kinetic attacks, traditional deterrence theory does not work for these attacks. Accordingly, policymakers need to focus on improving defense and dissuasion.

POLICY RECOMMENDATIONS

Implementing deterrence against kinetic attacks in space requires a tacit understanding of thresholds, and threatened responses of crossing those thresholds, both of which require engagement between senior policymakers from the countries involved.[40] This communication must include specifics. The 2010 United States National Space Policy says that to prevent aggression in space "[t]he United States will employ a variety of measures…".[41] This vague

language does not demonstrate resolve nor unambiguously articulate the costs associated with an attack in space. While the implied flexibility can be good, it does not communicate an effective deterrent. Also, the latest national security strategy states that "[a]ny harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing."[42] Though this broad statement gives policymakers wide-ranging options to respond to an attack, it is not an effective deterrent. An adversary does not understand what action would induce a response nor what that response is; thus, there is no impact on the adversary's cost-benefit calculation. Additionally, such a broad statement implies that policymakers have not sufficiently considered how to respond to an attack in space, lessening the perceived resolve to respond. To address these weaknesses, policymakers, namely the National Security Staff, in coordination with the Department of State, need to formulate and communicate specific responses to kinetic aggression in space.

Additionally, the National Security Staff needs to lead an effort to address non-kinetic physical, electromagnetic, and cyber attacks. Such an undertaking requires participation from a broad swath of government organizations and commercial companies from the United States and allied countries. At a minimum it must include the Departments of Defense, Commerce, Transportation, and Homeland Security, the National Aeronautics and Space Administration, launch service providers, and major U.S. based satellite operators. Intergovernmental organizations such as the International Telecommunication Union also need to be included. Topics for this group to address include hardening requirements for military, civil, and commercial spacecraft as well as clear expectations and delineation of responsibilities between allied governments and between governments and civilian companies. Methods to attribute,

defend against, and dissuade such attacks also need to be developed. A longer-term goal should be to extend the theory and practice of deterrence to these types of attacks, either in its traditional form, or in a new manner which may mirror deterrence in cyberspace.

Further, policymakers need to develop international norms and expand coordination mechanisms to prevent inadvertent escalation. In fact, due to the remoteness of space, the low maturity of space situational awareness, and the expanding number of actors in space, the risk of inadvertent escalation is higher in the modern space age than it was during the Cold War.[43] The Washington-Moscow Direct Communications Link and the United States-Soviet Incidents at Sea agreement serve as models of coordination mechanisms and norms.[44] With the expansion of cyberspace, new international norms must account for not only physical interaction in space, but also the intersection of space and cyberspace. While deterrence in cyberspace has many challenges,[45] coordination mechanisms and international norms can help reduce the likelihood of inadvertent escalation. However, unlike Cold War constructs, space coordination mechanisms and norms must extend to more countries, as well as to companies that launch and operate satellites, of which many are multinational corporations. This integration across governments and commercial companies will require innovative solutions that balance security, business interests, and the long-term utility of space. Finally, norms and coordination mechanisms must be codified and communicated to a broad audience in order to reduce ambiguity. Words, however, are not enough.

Exercises, both space- and terrestrial-based, can help convey capability and resolve.[46] Such exercises should include satellite anomaly resolution, attribution, and a simulated response. While such exercises may improve readiness within the American military, they can also be a communication mechanism with adversaries. Some undisclosed capabilities will need to be

revealed, much like the Air Force did in 2014 when it disclosed the existence of the Geosynchronous Space Situational Awareness Program.[47] Adversaries must believe that the United States can attribute an attack and has the capability and resolve to impose sufficient costs if a satellite is attacked. Only then will deterrence affect adversary behavior.

Finally, even if policymakers decide that preventing aggression in space through deterrence is the right path, it will be a challenge to execute within the United States' budgetary process. Deterrence is in the mind of an adversary thus its effectiveness is not easy to measure.[48] Accordingly, it will be hard to justify expenditures to deter aggression since the measure of success is the lack of an attack. However, policymakers need to build space deterrence into the budgeting process, with a focus on space situational awareness. Space situational awareness is an integral part of deterring aggression due to its part in attributing an attack. While better space situational awareness will not deter non-kinetic physical, electromagnetic, and cyber attacks, it aids in the defense and dissuasion against such attacks. To that end, the United States and its allies are working to improve space situational awareness capabilities,[49] which will require near-term procurement authority as well as a long-term operations and sustainment budget. These improvements are both timely and necessary given that "…the need for situational awareness cannot be overstated."[50] Without improved space situational awareness, a war in space, along with its catastrophic effects, becomes more likely.

NOTES

1. Clifton Parker, "Deterrence in Space Key to U.S. Security," U.S. Strategic Command, January 24, 2017, http://www.stratcom.mil/Media/News/News-Article-View/Article/1059106/deterrence-in-space-key-to-us-security/.

2. "International Space Station Again Dodges Debris," *Orbital Debris Quarterly News* 15, no. 1 (2011): 1.

3. Michael Krepon and Julia Thompson, "Anti-Satellite Weapons, Deterrence and Sino-American Space Relations" (Naval Postgraduate School Center on Contemporary Conflict, 2013), 10.

4. "Satellite Collision Leaves Significant Debris Clouds," *Orbital Debris Quarterly News* 13, no. 1 (2009): 2.

5. Cheryl Pellerin, "Hyten: Deterrence in Space Means No War Will Be Fought There," U.S. Department of Defense, January 29, 2017, https://www.defense.gov/News/Article/Article/1061833/hyten-deterrence-in-space-means-no-war-will-be-fought-there/.

6. Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 12.

7. Todd Harrison et al., "Escalation and Deterrence in the Second Space Age" (Center for Strategic and International Studies, 2017), 3–4, https://www.csis.org/analysis/escalation-and-deterrence-second-space-age.

8. Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," *Science and Global Security* 17, no. 1 (2009): 21.

9. George and Smoke, *Deterrence in American Foreign Policy*, 11.

10. Ibid., 48.

11. Ibid., 21 & 48.

12. Forrest E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, vol. MG-916-AF (Santa Monica, CA: RAND Corp, 2010), 14, https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG916.pdf.

13. Ibid.

14. Krepon and Thompson, "Anti-Satellite Weapons, Deterrence and Sino-American Space Relations," 51.

15. “National Security Decision Making: Security Strategies-4: Deterrence Theory and Nuclear Weapons,” n.d.

16. Krepon and Thompson, “Anti-Satellite Weapons, Deterrence and Sino-American Space Relations,” 28.

17. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 10–16.

18. Ibid., 12.

19. Krepon and Thompson, “Anti-Satellite Weapons, Deterrence and Sino-American Space Relations,” 10.

20. Ibid., 94.

21. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 12–15.

22. Ibid., 16.

23. Andrea Shalal-Esa, “U.S. Still Probing Security Satellite Failure,” *Reuters*, January 6, 2009, https://www.reuters.com/article/us-northrop-satellite/u-s-still-probing-security-satellite-failure-idUSTRE5055DW20090106.

24. Ibid.

25. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 43.

26. Ibid.

27. John B Sheldon, “Space Power and Deterrence: Are We Serious,” *Policy Outlook (Washington, DC: The George C. Marshall Institute* 1 (2008): 4.

28. Joshua M Epstein, “Horizontal Escalation: Sour Notes of a Recurrent Theme,” *International Security* 8, no. 3 (1983): 19.

29. Parker, “Deterrence in Space Key to U.S. Security.”

30. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 43.

31. George and Smoke, *Deterrence in American Foreign Policy*, 31.

32. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, n.d., sec. III, http://disarmament.un.org/treaties/t/outer_space.

33. Uri Tor, “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence,” *Journal of Strategic Studies* 40, no. 1–2 (2017): 93, https://doi.org/10.1080/01402390.2015.1115975.

34. Karen Parrish, “Official Describes Evolution of Space Deterrence” (Washington: Federal Information & News Dispatch, Inc, September 19, 2013), http://archive.defense.gov/news/newsarticle.aspx?id=120818.

35. Epstein, “Horizontal Escalation: Sour Notes of a Recurrent Theme,” 24.

36. Krepon and Thompson, “Anti-Satellite Weapons, Deterrence and Sino-American Space Relations,” 61.

37. Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 111.

38. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 7.

39. Krepon and Thompson, “Anti-Satellite Weapons, Deterrence and Sino-American Space Relations,” 76.

40. Ibid., 63.

41. “National Space Policy of the United States of America” (Executive Office of the President, Washington, D.C., June 28, 2010), 3, https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.

42. Donald Trump, “The National Security Strategy of the United States of America” (Executive Office of the President, Washington, D.C., December 2017), 31.

43. Harrison et al., “Escalation and Deterrence in the Second Space Age,” 29.

44. Johnson-Freese, *Space as a Strategic Asset*, 247.

45. Clorinda Trujillo, “The Limits of Cyberspace Deterrence,” *Joint Force Quarterly : JFQ*, no. 75 (2014): 47–50.

46. Sheldon, “Space Power and Deterrence: Are We Serious,” 4.

47. Pellerin, “Hyten.”

48. Sheldon, “Space Power and Deterrence: Are We Serious,” 1.

49. Parrish, “Official Describes Evolution of Space Deterrence.”

50. Johnson-Freese, *Space as a Strategic Asset*, 111.