Information Brownouts: Deterrent Threats on Infrastructure in Space

January 2023

Siddharth Manay

Center for Global Security Research

LAWRENCE LIVERMORE NATIONAL LABORATORY

Information Brownouts: Deterrent Threats on Infrastructure in Space

Siddharth Manay[1]

Lawrence Livermore National Laboratory

Executive Summary

The concept of deterrence matured in the 1950s and 1960s, mostly focused on preventing the use of nuclear weapons. Currently, the defense community believes that deterrence thinking can be applied across many types of State behavior, both military and non-military. This includes traditional military domains like land, sea, and air; non-traditional military domains like space and cyber; and non-military domains like economics and trade. The orchestrated use of all these domains to achieve a strategic effect is integrated strategic deterrence.

As part of the effort to establish integrated strategic deterrence, the United States seeks to develop concepts for imposing costs on an adversary that would change their calculus. The methods for imposing these costs should be drawn from all the tools at the nation's disposal, not just the implicated domain. While nuclear employment remains the ultimate in cost imposition, it is disproportionate in most crises and conflict situations. Policymakers look to other domains (conventional, cyber, space, economic, diplomatic) for a menu of flexible options that can be tailored to the conflict, stakes, and adversary.

Once the deterrence aperture is opened to include many domains, questions about deterring across domains naturally follow. Must cross-domain deterrence be structured pairwise between domains, or can a threat in one domain deter actions in several others?

This work focuses on whether threats of cost-imposition in one domain, space, can be used to deter adversary behavior in other domains, such as conventional. If so, what Blue counterspace threats would have a deterrent effect, and what Red actions could be deterred? The logic of these tools for cross-domain and multi-domain deterrence has not been explored; this exploration is needed if policymakers are going to be able to rely on them.

This paper argues that Blue counterspace threats against Red infrastructure in space are of limited value for deterrence by threats of punishment. This conclusion is based first on the costs imposed by a counterspace attack; namely, the damage or degradation of the service or capability.

These costs must then be balanced against the fact that Blue counterspace attacks result in additional pre-emption pressure on Red (and vice-versa); this is a side-effect that Blue must consider. Space-based infrastructure provides information, some of which is enabling for real-time military operations. The sudden absence of that information is a "brownout" that could be misperceived as a precursor to an attack. Because of this, the deterrent value of a counterspace threat will be highly dependent on the type of capability that the specific satellites are

[1] The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

supporting, and how badly that capability is degraded. Many counterspace threats may be deemed too small, degrading information capabilities in a way that will not impose much cost, because the information can be obtained in other ways or done without. Other counterspace threats may be deemed too large in that they are either not credible because Blue has not communicated the capability, or risky to Blue due to information brownout side effects.

Introduction

The concept of deterrence matured in the 1950s and 1960s, mostly focused on preventing the use of nuclear weapons.[2] Currently, the defense community believes that deterrence thinking can be applied across many types of State behavior, both military and non-military. This includes traditional military domains like land, sea, and air; non-traditional military domains like space and cyber; and non-military domains like economics and trade. The orchestrated use of all these domains to achieve a strategic effect is integrated strategic deterrence.[3]

Integrated strategic deterrence includes integration across several axes and concepts, including government, allies, domains, theaters, and spectrum of conflict.[4] Across government, the need is to use all instruments of government at the strategic level for competition, crises, and conflict. These instruments include military (ground, air, sea, nuclear, space, and cyber), political, diplomatic, economic, and civil mobilization. Decisionmakers need a menu of threats to use against adversaries to advance U.S. interests in crises or conflicts.[5] For military domains, decisionmakers need competent, effective, integrated military defense/denial capabilities that are credible to the enemy.[6]

As part of the effort to establish integrated strategic deterrence, the United States seeks to develop concepts for imposing costs on an adversary that would change their calculus. The methods for imposing these costs should be drawn from all the tools at the nation's disposal, not just the implicated domain. Nuclear employment remains the ultimate form of cost imposition but is disproportionate in most crises and conflict situations. Policymakers look to other domains (conventional, cyber, space, economic, diplomatic) for a menu of flexible options that can be tailored to the conflict, stakes, and adversary.[7]

---

[2] L. Freedman, *Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981).

[3] For the use and definition of the phrase, see L.J. Austin, Speech at the Fullerton Lecture Series in Singapore (July 27, 2021). https://www.defense.gov/News/Transcripts/Transcript/Article/2711025/secretary-of-defense-lloyd-j-austin-iii-participates-in-fullerton-lecture-serie/. Accessed August 23, 2022. But the concept has been around in some form; see the "full symphony of American power" in (Gates, 2020); "Soft power" in the Obama era; and arguably gunboat diplomacy and Theodore Roosevelt's "big stick" diplomacy.

[4] J. Garamone, "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says," DOD News (December 8, 2021). https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/. Accessed October 4, 2022.

[5] M. Chase and A. Chan, *China's Evolving Approach to "Integrated Strategic Deterrence"* (Santa Monica: RAND Corp., 2016), p55.

[6] My read of Chase and Chan, *China's Evolving Approach to "Integrated Strategic Deterrence,"* Chapter 3.

[7] B. Radzinsky, et al., "Setting Priorities for Deterrence Integration," Workshop Summary, Center for Global Security Research (2021).

Once the deterrence aperture is opened to include many domains, questions about deterring across domains naturally follow. Can threats, postures, or signals in the cyber domain, for instance, deter an adversary's conventional actions? Further, must cross-domain deterrence be structured pairwise between domains, or can a threat in one domain deter actions in several others?

These questions are vast and are the subject of ongoing study, discussion, and application. This work focuses on whether threats of cost-imposition in one domain, space, can be used to deter adversary behavior in other domains, such as conventional. If so, what Blue counterspace threats would have a deterrent effect, and what Red actions could be deterred? The remainder of this paper discusses whether counterspace tools can be used to impose costs and what factors contribute to the amount of such costs. These concepts are developed abstractly at first and then applied to example scenarios where the additional marginal cost may change the adversary's calculus.

This question is relevant to the policymaking community for several reasons. First, the balance of U.S. assets in space, when compared to any other spacefaring nation, shows that the U.S. economy and military are highly reliant on space infrastructure and are therefore asymmetrically vulnerable to attacks in space.[8] This seems to be a sticking point in the debate about counterspace attacks, based on the assumption that any U.S. counterspace attack would be met with retaliation—resulting in the United States paying the higher cost in the exchange. This ignores the fact that Red does pay costs while the United States does have resilience. Second, U.S. policymakers need deterrence tools below the nuclear threshold, and space and cyber tools are frequently seen as alternatives that are effective and more proportionate. However, the logic of these tools for cross-domain and multi-domain deterrence has not been explored; this exploration is needed if policymakers are going to be able to rely on them.[9]

---

[8] B. Bahney, J. Pearl, and M. Markey, "Antisatellite Weapons and the Growing Instability of Deterrence," in J. R. Lindsay, & E. Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019).

[9] P. Bernstein and A. Long, "Multi-Domain Deterrence: Some Framing Considerations," in B. Roberts, ed., *Getting the Multidomain Challenge Right* (Livermore, CA: Center for Global Security Research, 2021), p6; P. Bernstein, "Toward an Integrated Strategic Deterrent," in B. Roberts, ed., *Fit for Purpose? The U.S. Strategic Posture in 2030 and Beyond* (Livermore, CA: Center for Global Security Research, 2020), p76; B. Bahney and J. Pearl, "The Challenge of Integrating Space and Cyber into U.S. Security Thinking," in B. Bahney, ed., *Space Strategies at a Crossroads* (Livermore, CA: Center For Global Security Research, 2020), pp58-62. The U.S. strategy in cyberspace is mature; see U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed November 21, 2022; *National Cyber Strategy of the United States of America* (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed November 21, 2022; M.P. Fischerkeller, *What Do We Know About Cyber Operations During Militarized Crises?* (2022), Atlantic Council; M.P. Fischerkeller and R. J. Harknett, *Initiative Persistence as the Central Approach for U.S. Cyber Strategy* (2021). Institute for Defense Analyses, https://www.ida.org/-/media/feature/publications/i/in/initiative-persistence-as-the-central-approach-for-us-cyber-strategy/d-22719.ashx, accessed November 21, 2022; R. Harknett and M. Smeets, "Cyber Campaigns and Strategic Outcomes: The Other Means," *Journal of Strategic Studies* (March 2020), doi: https://doi.org/10.1080/01402390.2020.1732354, accessed November 21, 2022; T. Rid, "Think Again: Cyberwar," *Foreign Policy* (2012), http://foreignpolicy.com/2012/02/27/think-again-cyberwar, accessed November 21, 2022; J.G. Schneider, "Deterrence in and Through Cyberspace," in J. R. Lindsay and E. Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity*, (Oxford: Oxford University Press, 2019), pp95-120. The U.S. strategy to deter attacks on U.S. assets in space are discussed in F.E. Morgan, Deterrence and First-Strike Stability in Space: A Preliminary Assessment (Santa Monica, CA: Rand Corporation, 2010), https://www.rand.org/pubs/monographs/MG916.html, accessed November 21, 2022; and B. Bahney, J. Pearl, and M. Markey,

In this work, while the Blue action is restricted to one domain, the desired effect is cross- and multi-domain. This analysis alone does not result in integrated deterrence, but if such one-to-many costs can be imposed, it suggests 1) that space is one option on the decisionmakers' menu of deterrent threats that can be applied regardless of the domain Red is working in, and 2) costs imposed in and through other domains may have the same utility. Further, the costs and benefits of a single-domain attack, understood in isolation, are the foundation of understanding the synergies between a coordinated attack in multiple domains. This evaluation, then, is a step towards and component of practical integrated deterrence.

To frame the question, this paper considers the case of a crisis or conflict between the United States and China, likely in and around Taiwan and the South China Sea. This pairing is chosen because the United States and China both:

- are Great Powers
- are nuclear armed
- have formidable conventional militaries
- have space infrastructure that their militaries rely on to some degree
- have counterspace capabilities.

To address cross-domain deterrence, the example scenarios in this paper are not limited to deterring a specific action in a specific domain; rather, the article explores the features and effects of counterspace threats before analyzing the deterrent effect against a range of example Red actions.

The argument presented here is that Blue counterspace threats against Red infrastructure in space are of limited value for deterrence by threats of punishment. This conclusion is based on the costs imposed by a counterspace attack. A non-reversable counterspace attack would damage an asset in space, imposing the immediate cost of the losing the asset. This cost alone is not high in relation to a crisis or conflict where regional or national interests, not to mention lives and military hardware, are at stake. However, the costs are not limited to the asset itself, as the asset supports a larger service or capability. The damage or degradation of that service or capability is the large and more salient cost imposed on Red.

These costs must be balanced against the fact that Blue counterspace attacks result in additional pre-emption pressure on Red (and vice-versa); this is a side effect that Blue must consider. Space-based infrastructure provides information, some of which is enabling for real-time military operations. The sudden absence of that information is a "brownout" that could be misperceived as a precursor to an attack. Because of this, the deterrent value of a counterspace threat will be highly dependent on the type of capability that the specific satellites are supporting, and how badly that capability is degraded. Many counterspace threats may be deemed too small, degrading information capabilities in a way that will not impose much cost,

"Antisatellite Weapons and the Growing Instability of Deterrence" (2019). But none of these works explores the use of cyber or space to deter attacks *outside those domains.* However, N. Kostyuk and Y.M. Zhukov (n.d.), *Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?*, https://scholar.harvard.edu/zhukov/publications/invisible-digital-front-can-cyber-attacks-shape-battlefield-events, accessed March 2022, does discuss the possibility of cyberattacks affecting battlefield events.

because the information can be obtained in other ways or done without. Other counterspace threats are may be deemed too large in that they are either not credible because Blue has not communicated the capability, or risky to Blue due to information brownout side effects.

The next few sections briefly review the classic deterrence framework as it is applied here, the literature on deterrence in space, the capabilities supported by space infrastructure, and U.S. counterspace capabilities. The connection between counterspace attacks, information brownout, and pre-emption pressure are discussed. With these baselines, the next step is to evaluate the cost to Red—and the side-effects to Blue—of different types of counterspace attacks. These factors are based on the features of the capability targeted: What was it? How does losing it affect Red? What is the magnitude of degradation or damage done? How resilient is Red to its loss? Each capability must be evaluated on a case-by-case basis, which is done in tabular format with a discussion.

Deterrence and Space

Deterrence

This section briefly reviews the concepts of deterrence in broad strokes to frame the logic for counterspace threats.

Deterrence is generally defined as actions that would change an adversary's calculus, convincing them not to act when they otherwise might have.[10] The logic is frequently explained in terms of the cost and benefit of the adversary action, considered from that adversary's point of view. Deterrence works by attempting to change these two quantities: cost and benefit. The key factor here is the change in the adversary's perceptions of cost and benefit. To isolate the deterrent effect, first note that the adversary has an *a priori* set of costs and benefits it expects from taking the action. These are already "baked in" and should not be confused with the deterrent effect.

Two main mechanisms for deterrence are denial and punishment. Deterrence by denial mainly affects the benefit side of the balance, reducing the likelihood that the adversary can achieve a gain (or diminish the amount of gain). Deterrence by punishment mainly affects the adversary's cost by threatening to add to those costs deliberately and actively.

For cross-domain deterrence, the denial mechanism is straightforward. If Blue's counterspace posture presents a credible capability to undermine Red's action in another domain, then Red (assuming rationality, good information, and clear perception) will have already considered its reduced likelihood of success as part of their benefit calculation. The deterrence flows from the Blue capability to deny and takes effect at the time Blue obtains this capability. This is a tool

[10] P.M. Morgan, "The Past and Future of Deterrence Theory," in J.R. Lindsay and E. Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019); L. Freedman, *Evolution of Nuclear Strategy (*New York: St. Martin's Press, 1981); J.J. Mearsheimer, *Conventional Deterrence* (Ithaca and London: Cornell University Press, 1983); United States Strategic Command, Director Plans and Policy, *Deterrence Operations Joint Operating Concept*, Department of Defense (2006), https://apps.dtic.mil/sti/pdfs/ADA490279.pdf, accessed November 10, 2022.

and posture that decisionmakers invest in well ahead of the conflict, but it will not be the tool that decisionmakers deploy in real time to a crisis or conflict. Further, the deterrent effect is somewhat stove-piped, as the Blue deterrent capability can only deny those actions where there's a causal link in the physical world. For example, Blue artillery can stop a tank. A Blue cyberattack may also slow a tank, but only to the extent the tank relies on real-time digital software and information and can be made less effective by a disruption in that information. Therefore, artillery can play a clear role in deterrence by denial of a Red decision to act with tanks; a cyber capability may play a role as well, but one that is much less clear and much less certain. Without such a link, deterrence by denial cannot work. For this reason, this article does not focus on deterrence by denial.

Punishment, on the other hand, is somewhat less time- or domain-constrained. The threat to punish in a specific way, in retaliation for a specific Red action, is something decisionmakers can communicate during a crisis or conflict, assuming the capability and posture exist. Further, the punishment does not have to be causally linked to Red's action; for instance, Blue can threaten economic sanctions in retaliation against Red's decision to act with tanks. Unlike the causal, physical linkage required for deterrence by denial, deterrence by punishment is always linked by a common, psychological logic of pain. (To imagine this, set aside for a moment the complexities of communicating the threat and the psychological linkage of action and threat in the minds of Red's decisionmakers.) For this reason, cross-domain actions provide more opportunities for punishment threats.

To apply to counterspace actions in a crisis, this paper assumes that the United States is already postured for all the military (conventional, cyber, etc.) denials that U.S. counterspace capabilities can access, and that China has already considered these capabilities in its cost-benefit analysis. In the midst of the crisis or conflict, faced with possible escalation by China, the tools remaining to U.S. decisionmakers are threats of punishment. The typical form of such a threat would be a signal or communication that the United States will degrade or destroy some number and type of Chinese satellites in retaliation for some action China is considering. The remainder of this paper discusses whether counterspace tools can be used to impose costs in this way, estimate the cost, and outline cases where the additional marginal cost may change the adversary's calculus.

Deterrence in the Space Domain

Much of the scientific and commercial use of space was secondary to the military use of rocketry (for ballistic missiles) and space [for intelligence, surveillance, and reconnaissance (ISR)]. The primary modern use of space is as a useful location to mount tools on unmanned satellites in orbit. These tools consist of information-gathering devices, such as cameras and detectors used for everything from meteorology, land-use characterization, other commercial purposes, and ISR; information-relay devices to transmit radio signals, television signals, and digital information; and, uniquely, a source of position, navigation, and timing (PNT) information implemented as global navigation satellite systems (GNSSs), namely GPS, Galileo,

GLONASS, and BeiDou. All these purposes have military application, and several states rely on these services for military operations.[11]

The military and economic importance of these systems gives states an incentive to attack their adversaries' satellites to gain an advantage, especially in a crisis; in turn, this raises the question of how a state can defend its satellites from attack or deter attacks. As they orbit around Earth at varying altitudes, these systems are somewhat brittle and difficult to defend. Because of this, much of the analysis and writing on space deterrence has focused on how a state—especially the United States—might defend from attack and especially deter an attack.[12] Deterrence is difficult and setting norms about the use of space is one crucial path to minimizing the United States' exposure.[13]

There is less written about a state holding an *adversary's assets in space* at risk to deter the adversary from taking action. When this side of the coin is discussed, authors are quick to note that the United States has the largest number of assets in space, and the United States' expeditionary military has the longest history of dependence on infrastructure in space. Because of this, authors reason, the United States has the most to lose in a tit-for-tat exchange of counterspace strikes and retaliatory responses.[14] This ignores the fact that the adversary does have assets in space that it also stands to lose, and that the current balance may shift as other states, especially China, continue to catch up. The purpose of this paper is to take another look at the strategy of holding Red's assets at risk, and the possible costs and benefits of doing so.

Assets and Targets in Space

In general, satellites in space are information technology infrastructure, focused on gathering and moving information for civilian and military purposes.[15] To provide more context, military infrastructure can be further divided into strategic (nuclear) infrastructure and conventional

---

[11] United States Air Force, Curtis E. Lemay Center for Doctrine Development and Education, *Counterspace Operations.* Air Force Doctrine Publication, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf, accessed September 28, 2022; Defense Intelligence Agency, *Challenges to Security in Space* (2019), https://www.defense.gov/News/News-Stories/Article/Article/1754509/dia-report-details-threats-to-americas-space-based-world/2019, accessed November 21, 2022; Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, *Space Domain Mission Assurance: A Resilience Taxonom*y (2015).

[12] M. Stokes, G. Alvarado, E. Weinstein, and I. Eason, *China's Space and Counterspace Capabilities and Activities,* Project 2049 Institute (2020), https://www.uscc.gov/research/chinas-space-and-counterspace-act, accessed 2022; F.E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (Santa Monica, CA: RAND Corporation, 2010), https://www.rand.org/pubs/monographs/MG916.html, accessed February 2022; B. Bahney, J. Pearl, and M. Markey, "Antisatellite Weapons and the Growing Instability of Deterrence" (2019); A. Astorino-Courtois, R. Elder, and B. Bragg, *Contested Space Operations, Space Defense, Deterrence, and Warfighting: Summary Findings and Integration Report* (Boston: NSI, Inc., 2018), https://apps.dtic.mil/dtic/tr/fulltext/u2/1066708.pdf, accessed November 21, 2022.

[13] F.E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (2010).

[14] B. Bahney, J. Pearl, and M. Markey, "Antisatellite Weapons and the Growing Instability of Deterrence" (2019); F.E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (2010).

[15] B. Bahney and J. Pearl, "Why Creating a Space Force Changes Nothing," *Foreign Affairs* (2019), https://www.foreignaffairs.com/articles/space/2019-03-26/why-creating-space-force-changes-nothing, accessed November 21, 2022.

infrastructure, while the information services provided are Position, Navigation, and Timing (PNT); Intelligence, Surveillance, and Reconnaissance (ISR); Command, Control, and Communications (C3); and Meteorology.

The civilian part of these applications supports commerce, government, and health and safety. As such, degrading or destroying these capabilities can impose some pain on the population, including economic costs and lives lost indirectly (for example, if first responders and medical facilities are hobbled). The military part of these applications supports conventional actions on land, sea, and air, as well as intelligence, targeting, precision strike, force projection, and logistics. Degrading or destroying these capabilities will in turn degrade military effectiveness, either in the short term (for example, decreased accuracy of a missile) or long term (that is, reduced intelligence which limits targeting opportunities or increases the vulnerability to a surprise attack). This degradation may in turn leave a state fearful that their military denial capabilities are weakened and shake its confidence that the adversary has been deterred. The strategic applications are nuclear targeting, nuclear command and control (NC2), nuclear early warning, and nuclear guidance. Degrading these can diminish the readiness and effectiveness of nuclear employment, which in turn may reduce a state's confidence in its survivable second-strike capability—therefore creating some pre-emption pressure.[16]

Understanding the downstream effects of a counterspace attack is complicated by the fact that a country's space infrastructure may be of dual use. Civilian and military, or military and nuclear capabilities, may be commingled on a single platform. In this case, a counterspace attack would have all the effects, positive and negative, of attacking both sets of infrastructure. However, confident intelligence on the purposes of a space asset is needed before making the decision to degrade or destroy.

Resilience is a crucial consideration for a state that relies on space infrastructure (and indeed all infrastructure), and therefore for counterspace attacks on that infrastructure.[17] Resilience can come in several forms. One form is duplication redundancy, implemented as several (or a constellation) of satellites that perform the same function, so that the loss of some of these satellites does not mean the complete loss of the function. [This conflates the Department of Defense (DOD) concepts of disaggregation, distribution, and proliferation.] Another form is substitution redundancy, this time implemented as, or resulting from, an alternate type of infrastructure that serves a similar function, such as terrestrial communications links that work alongside satellite communications (SATCOM) or the alternate guidance methods used by some

[16] B. Bahney, "The Changing Role of Space in the U.S. Strategic Posture" in B. Roberts, ed., *Fit for Purpose? The U.S. Strategic Posture in 2030 and Beyond* (Livermore, CA: Center for Global Security Research, 2020), p67; C. Talmadge, "Would China Go Nuclear?: Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (2017), pp50-92.

[17] This article uses the term "resilience" to mean "ability of a *capability* to resist degradation, return to service after degradation, or function despite degradation." This is an informal, loose usage, and focused on mission assurance (the capability) instead of system assurance (the satellite). This usage deviates from DOD taxonomy, which focuses on the satellite; distinguishes defensive operations, reconstitution, and resilience; and further expands resilience into disaggregation, distribution, diversification, protection, proliferation, and deception. See Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, *Space Domain Mission Assurance: A Resilience Taxonomy* (2015).

precision weapons.[18] (This is related to DOD's concept of diversification.) A third form is simply doing without. For instance, a state may target fixed targets in the absence of ISR satellites by using existing intelligence. In all these cases, the loss of a small number of satellites imposes costs in the form of some amount of decreased efficiency, but not the inability to perform.

China is a space power with active military and civilian space programs (both run by the same agency). They employ infrastructure in space for civilian, military, and strategic applications.[19] Many of these assets are dual-use.[20] Military application includes conventional military operations around Taiwan or in the South China Sea, where PNT, ISR, and C3 will support joint operations.[21] Many Chinese applications have some degree of resilience, including resilience from a constellation (there are 35 BeiDou PNT satellites) and from substitution redundancy (terrestrial and radio links are likely their primary source of communications, as these conflicts are close to the Chinese mainland).

Counterspace Capabilities

Counterspace capabilities take many forms, including attacks on the satellite itself or attacks on the infrastructure that supports the satellite. The attacks can be kinetic or non-kinetic, and reversible or non-reversible.[22] This range of options, many of them "soft" and few involving attacks on an adversary's homeland or the loss of life, is what makes counterspace (and similarly cyber) attacks seem attractive to policymakers.

Open sources make scant reference to existing U.S. counterspace tools.[23] There are mentions of the feasibility of adapting systems with other purposes to counterspace uses, such as ballistic missile defense capabilities adapted to direct-ascent kinetic attacks and directed energy

[18] In 2022, Starlink countered communications jamming with "one line of code" S. Losey, "SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month—and the Pentagon is taking notes," C4ISRNET (April 20, 2022), https://www.c4isrnet.com/air/2022/04/20/spacex-shut-down-a-russian-electromagnetic-warfare-attack-in-ukraine-last-month-and-the-pentagon-is-taking-notes/, accessed May 5, 2022.

[19] E. Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017* (Santa Monica, CA: RAND Corporation, 2015), Chapters 9 and 10; M. Chase and A. Chan, *China's Evolving Approach to "Integrated Strategic Deterrence"* (Santa Monica: RAND Corp., 2016), Chapter 3.

[20] C. Talmadge, "Would China Go Nuclear?: Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States" (2017); M. Stokes, G. Alvarado, E. Weinstein, and I. Easton, *China's Space and Counterspace Capabilities and Activities* (2020); T. Zhao and L. Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective," in J. M. Acton, A. D. Arbatov, P. Topychkanov, T. Zhao, and L. Bin, *Entanglement: Chinese and Russian Perspectives on Non-nuclear Weapons and Nuclear Risks* (Washington DC: Carnegie Endowment for International Peace, 2017), https://carnegieendowment.org/2017/11/08/underappreciated-risks-of-entanglement-chinese-perspective-pub-73164, accessed August 23, 2022.

[21] M. Stokes, G. Alvarado, E. Weinstein, and I. Easton, *China's Space and Counterspace Capabilities and Activities* (2020); T. Harrison, K. Johnson, J. Moye, and M. Young, *Space Threat Assessment 2021* (2021), CSIS Aerospace Security Project, https://www.csis.org/analysis/space-threat-assessment-2021, accessed 2022.

[22] Defense Intelligence Agency, *Challenges to Security in Space* (2019), https://www.defense.gov/News/News-Stories/Article/Article/1754509/dia-report-details-threats-to-americas-space-based-world/, accessed 2022.

[23] In open literature, the only offensive capability is the "Meadowlands, a mobile, terrestrial-based, counter-communications system (CCS)." J Venable, *An Assessment of U.S. Military Power: U.S. Space* Force (2021), Heritage Foundation, https://www.heritage.org/military-strength/assessment-us-military-power/us-space-force 2021, accessed October 14, 2022.

weapons for reversible attacks.[24] They seem few in number and are not frequently demonstrated or publicly exercised.[25] There seems to be little information about the posture of these assets, such as the positioning of counterspace weapons globally to threaten spacecraft in geosynchronous orbit. This is due to the U.S. desire to protect information about those assets, set norms about the uses of space, and prevent an arms race. These are sound reasons with positive impacts on U.S. national security, but they may result in the perception that the United States has little ability to credibly either threaten to deny an adversary's action in space or threaten an adversary with counterspace attacks.

Special Consideration for Counterspace Attacks: Information Brownout

A crucial consideration for counterspace attacks is the recognition that Blue's attack would degrade or destroy Red's information infrastructure. The primary effect may be the degradation of the civil, military, or strategic infrastructure that depends on the targeted infrastructure component. [26] A secondary effect, however, will be Red's perception that it now has an information "brownout" that results in a gap in its situational awareness.[27] Red is likely to consider the fact that such a gap creates a virtual smokescreen that may enable a Blue attack. This increases the likelihood of misperception and pre-emption pressure, which in turn increases the likelihood of escalation, contrary to Blue's intention to manage escalation. This is in addition to the potential for misperceptions and incentives for pre-emption that already existed due to the nature of the crisis. If Blue is restrained and chooses not to use a counterspace attack, the existing potentials and incentives do not change, and escalations may still occur. The same is true in reverse; a Red counterspace attack on Blue information infrastructure in space would create the same potentials and incentives. However, this article focuses on Blue's ability to deter Red.

The type of capability degraded, and the magnitude of the degradation, will contribute to Red's evaluation of its vulnerability. This is not to be confused with the degradation or destruction of the satellite; this is focused on the overall capability (that is, the service provided by the system of satellites).

A rough taxonomy of the magnitude of degradation will help clarify the discussion:[28]

---

[24] Heginbotham, et al., 2015.

[25] *Ibid.*; T. Hitchens, "U.S. Pledges No Destructive ASAT Missile Tests, Urges International Norm," Breaking Defense (April 18, 2022), https://breakingdefense.com/2022/04/us-pledges-no-destructive-asat-missile-tests-urges-international-norm/, accessed July 14, 2022.

[26] B. Bahney, J. Pearl, and M. Markey, "Antisatellite Weapons and the Growing Instability of Deterrence" (2019); B. Bahney, "The Changing Role of Space in the U.S. Strategic Posture" (2020).

[27] The term "blackout," while more common, implies a complete lack of information. "Brownout" more accurately implies the more realistic case of a partial lack of information. Manzo refers to this as leaving the enemy "blind, deaf, and dumb." V. Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" *Joint Forces Quarterly* 66 (2012), pp45-60.

[28] This is a looser approach than the one in Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (2020), report to Congress, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF, accessed February 2022. It also elides the "Disrupt," "Deny," "Degrade,"

Minor degradation. Minor degradation is a level of degradation that is detectable by Red but has little impact on the overall capability Red is relying on. For example, the destruction of one or two BeiDou satellites would have very little effect on overall PNT services, as PNT frequently relies on signals from several of the 35 satellites.

Medium degradation. Medium degradation is a level that confounds Red's ability to function effectively. Information that it relies on is either missing in small quantities or is lower in quality. Examples include the destruction of enough BeiDou satellites to reduce the accuracy of units and weapons by amounts that make them less certain of their effectiveness; there are gaps in their real-time situational awareness due to degraded ISR or C3 capabilities.

High degradation. High degradation is a level that deeply undermines Red's ability to function. Information it relies on is missing entirely or is of very low quality. Examples include attacks that leave Red forces unable to acquire PNT information, with large gaps in situational awareness, or highly uncertain C3. This effect is hard to achieve when services are provided by a constellation of satellites, like BeiDou. However, for capabilities provided by low numbers of unique satellites, such as geosynchronous communications nodes or a specialized ISR capability, the effect might be achieved with the destruction of one or two satellites.

From Red's point of view, in the first minutes and hours after the counterspace attack, Red may have limited information. It has the fact that the supported capability is not functioning; it may have some status and diagnostic information from the satellite. It will be working to determine the root cause of this change in status. Possible reasons will include an attack (reversible or non-reversible) on the satellite, terrestrial electronic jamming, attacks on ground stations (whether cyber or kinetic), a satellite malfunction, a space debris strike, space weather, or other natural or human causes. Technicians will be focused on diagnosing the issue to provide information to decisionmakers while simultaneously attempting to restore service. Decisionmakers will be attempting to understand the technical issues (itself a difficult task and rife with avenues for misunderstanding) while considering external factors such as the current status of ongoing political and military crises or conflicts, Blue's counterspace capabilities and posture, any intelligence or early warning about Blue counterspace actions, and the number of satellites affected. This information will be diffuse, spread among numerous people and agencies across the military and government. The intelligence may reside with one organization, the technical information about one service may lie with another, and technical information about a second service (if the attack is widespread) may be possessed by a third organization. All of these locations are likely separate from the decisionmaker. It may take hours to assemble the information to create a coherent picture of the cause of the failure and the intent of any actors involved.

During this period, Red is working to make decisions under high time pressure with a high degree of uncertainty. Uncertainties may include whether the outage was caused by a Blue attack or something else. If it was a Blue attack, there may be uncertainty about whether it was

"Destroy" taxonomy in U.S. Air Force, *Counterspace Operations* (2021). For purposes of a brownout and in the short term, the distinctions between temporary and permanent and impair and eliminate aren't relevant.

deliberate or accidental; whether it is reversible or not; and whether it was intended as a signal, punishment, or denial. During this period, there is further uncertainty about the contents of the information that the attacked system was designed to gather. The fog of war is now thicker as a direct consequence of Blue's action.[29]

Regardless of cause, intent, and its uncertainty about cause and intent, Red is faced with a dilemma during this time. The degraded capability may leave it more vulnerable to a Blue conventional or nuclear attack. Blue has the opportunity to attack, or more broadly change the conditions of the battlefield in its favor, with an increased chance of success. More than an having an opportunity, Blue has motive to do so. Further, from Red's perspective, Blue would have incentive to attack quickly after instigating the brownout to prevent Red from restoring or compensating for the missing information, preparing a defense, or preempting Blue's attack. Red must consider this possibility and consider taking steps to mitigate the damage. Such steps could include raising the alert level of conventional or nuclear forces, rapid maneuvers, and pre-emptive conventional attacks.[30] Raised alert levels alone are enough to increase the risk of Blue misperception and inadvertent escalation.[31]

This skepticism about the cause may persist even if Blue has communicated the action and intent ahead of time. Red will need to consider the likelihood that Blue's assurance is simply a pretext to cover for a Blue attack that exploits the vulnerability. Consider the analogous case of a state that mobilizes its conventional army within its borders—but near the border with an adjacent country. No number of assurances that the mobilization is "just an exercise" will completely assuage the adjacent country's fears of an invasion.

The possibility of misperceived intent cuts multiple ways. As discussed above, Red may perceive a punishment counterspace attack as a first salvo in a broader conventional attack. Red may also perceive an accident or malfunction involving its satellite as a first salvo. The state of the crisis and the existence of Blue counterspace capabilities mean Red must consider the possibility that what is actually a malfunction is a deliberate Blue attack. Any Blue communications or signals threatening a punishing counterspace attack that happens to coincide with a malfunction will only increase Red's certainty that the outage is not an accident.

To be clear, an information brownout is the product of a counterspace attack that degrades Red's information capabilities. (It is arguably also a product of some cyberattacks, but that is beyond this scope of this paper.) The extent and duration of the brownout can be varied based on the choice of satellites, the number of satellites, and the type of counterspace attack (temporary vs. permanent; impair vs. eliminate[32]). If Blue's tactical or strategic need is *denial*, the brownout is the desired and useful product of the counterspace attack. But if Blue's

[29] T. Zhao and L. Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective" (2017).

[30] J. Dobbins, "War with China," *Survival* 7, no. 24 (2012) discusses this in a cyberattack context.

[31] F.E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (2010); T. Zhao and L. Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective" (2017).

[32] *Counterspace Operations* (2021).

strategic need is *punishment*, the brownout is a side effect of the counterspace attack, and therefore a risk to Blue.

In short, the information brownout from a medium or worse counterspace attack creates the conditions for misperception and gives Red incentive for conventional reaction and escalation.

"Leaving Something to Chance"

There is the possibility that the information brownout and possible escalatory reaction is a benefit. The potential for misperception and inadvertent escalation resulting from a counterspace brownout may be useful. From one perspective, conflicts, including military conflicts, are competitions in risk taking. In this approach, expounded by Thomas Schelling, conflict is first a bargaining process where both sides "bid" risk to show resolve and communicate the costs that the other side will likely endure. Further, a situation that exposes both sides to inadvertent or accidental escalation may leave Red with a higher perception of risk than any explicit threat Blue could make. Such risk has the benefit of not relying on Blue's credibility—that is, on Red's evaluation that Blue will actually follow through with a threat.[33]

A counterspace attack and the resulting brownout may have exactly this effect. A Blue counterspace attack and an information brownout leaves Blue forces protected behind a smokescreen while simultaneously signaling to Red that an attack is imminent. That is, Blue is giving Red incentive to attack. To the extent that Red realizes this and feels that its hand is being forced, this may seem to Red like precisely the kind of situation that leads to escalation. This perception may be sharpened by the all-domain context in which the brownout occurs; if a Blue carrier group is nearing a contested area and then Red suffers a brownout sufficient to create confusion about the position, direction, and capabilities of the group, Red is faced with a dilemma beyond the denial of its ability to confidently attack the carrier group. Red must also contend with the sense that it is being invited to attack the carrier group—inviting retaliation and further committing Blue to the conflict when it otherwise might not have.

A Blue *threat* of a counterspace attack and information brownout could potentially have a similar effect on Red. While the effect is less acute, Red may consider the results of such an attack and see the potential for misperception, accident, and inadvertent escalation.

For a Blue decisionmaker, such brownouts and brownout threats have the potential to be signals about the willingness to take risk and demonstrations of resolve. Applied judiciously, a counterspace attack that creates an information brownout, or the threat of such an attack, may have a deterrent effect, especially intra-conflict. However, being able to reliably generate this result seems unlikely. For that reason, this approach is not considered in the remainder of the paper.[34]

---

[33] T.C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008), pp92-125.

[34] Thank you to Jonathan Pearl, Ben Bahney, and Michael Markey for the conversation that generated these insights.

China

The previous section discussed perceptions and reactions that a space-faring great power may have in the wake of a punishing counterspace attack. How would China react?

China's doctrine is likely to create a mindset that a counterspace attack is a prelude to further attacks, and not a punishment alone. Its doctrine proscribes seizing the initiative, that is, reacting rapidly to a crisis to put the adversary on the defensive.[35] It further desires to manipulate the parameters of operations to shape circumstances in its favor.[36] These elements of doctrine may shape its perception of U.S. intentions as well as their reaction to those perceived intentions.

If they mirror these doctrinal elements onto the United States, Chinese decisionmakers could easily perceive a counterspace attack as an attempt by the United States to put China on the defensive and manipulate the parameters of the battlespace to the U.S.'s advantage. These perceptions may lead them to evaluate that the counterspace attack is a prelude and not solely a punishment. Even if they were uncertain in this evaluation, they are likely to at least consider the possibility.

Chinese decisionmakers may then desire to re-gain the initiative and change the battlespace to their advantage. This would require a rapid reaction of some kind, and not just acceptance of the brownout. Moreover, Chinese doctrine emphasizes escalation control and does not include discussion of inadvertent or accidental escalation.[37] These recommendations make it more likely that they would react without considering the possibility that they are miscalculating.

It is not possible to predict the reactions of Chinese decisionmakers in this situation. However, the desire and even pressure to react, and therefore escalate, is likely a factor in their decision making. U.S. decisionmakers will need to consider this possibility when considering counterspace punishment.

Evaluating Effects of Counterspace Punishment

The effect of a punishing attack on a country's space assets, and the capabilities they provide, is dependent on (among other things) the capability and the amount of degradation. This section explores that dependency.

The general framework for deterrence by punishment is first to consider a Blue action in retaliation for a possible future Red action. If that action is credible, then the threat of this

---

[35] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, 2020 (2020); F.E. Morgan, K.P. Mueller, E.S. Medeiros, K.L. Pollpeter, and R. Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (2008), pp47-75; B. Roberts, *On Theories of Victory, Red and Blue* (Livermore, CA: Center for Global Security Research, 2020); O.S. Mastro, "How China Ends Wars: Implications for East Asian and U.S. Security," *Washington Quarterly* 45, no. 60 (2018); and J. Dobbins, "War with China" (2012).

[36] F.E. Morgan, K.P. Mueller, E.S. Medeiros, K.L. Pollpeter, and R. Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (2008), pp47-75.

[37] *Ibid*.

action may be communicated or signaled to Red in an attempt to deter the Red action. Red will then consider the additional costs and risk imposed by the threat; if it finds the risk too high, it will be deterred. The desire of decisionmakers is that counterspace capabilities provide some deterrent threats below the nuclear-use threshold. As discussed previously, this evaluation is focused on deterrence by punishment, so neither the military denial benefits or the deterrence by denial possibilities are considered here. Also, the timing of the threat is assumed to be appropriate for the crisis or conflict. Threats of relatively low cost to Red are made early in the crisis, when sunk costs and stakes are low; threats of higher cost to Red are made later in the crisis when sunk costs and national stakes are higher.

To compare threats against information infrastructure, only the factors that differentiate the different capabilities are considered. In general, all these attacks signal some level of Blue resolve and a demonstration of a Blue capability. All these attacks would impose costs on Red, including the cost of replacement and the direct consequence of not having the capability provided by the infrastructure. And all attacks carry the risk that Red may decide to retaliate in kind against Blue. Were Blue to carry out any of these attacks, Blue would be breaking its own norms about the uses of space.

Table 1 summarizes the counterspace attacks that Blue can consider against Red. For each capability that Blue could target, the following are listed.

- Target Capability: the capability supported by the satellite.
    - Military and Civilian Position, Navigation, and Timing (PNT): PNT satellites, such as the 35-satellite BeiDou constellation.
    - Military Real-time ISR: Any satellite or constellation that provides (near) real-time ISR for situational awareness, battlespace awareness, or conventional early warning.
    - Military Specialized ISR: Satellites that provide unique ISR capabilities. These are assumed to be “exquisite” capabilities that are expensive to field, resulting in only 1-2 satellites with that capability. Because of their limited number, these are unlikely to be providing real-time intelligence, and are more likely to be providing information to planners.
    - Civilian ISR and Meteorology: Satellites that provide “surveillance” information and weather information. “Surveillance” likely takes the form of land-use, agricultural, and other ecological data (including systems like wildfire detection). Along with meteorology, these capabilities support commerce, government, and in some cases public safety.
    - Military or Civilian C3: Satellites that support over-the-horizon command and control. Assumes a constellation. For military satellite communications (also known as MILSATCOM), this focuses on coordination and situational awareness of forces. For civilians, this supports commerce, government, and emergency response.
    - Nuclear Command, Control and Communications (NC3) and Nuclear Early Warning (NEW): China is likely to consider any attack on these assets to be an attempt to degrade their assured second-strike capability.

- Degradation: The severity of the degradation to the capability caused by the attack. Note that reversibility and duration of the degradation are not considered here, for reasons discussed in the section titled "Special Consideration for Counterspace Attacks: Information Brownout"
- Cost imposed on Red: What cost will Red suffer if the attack is successful?
- Signals perceived by Red: Is there a likelihood that Red, having suffered a brownout, will perceive this as an attack?
- Risk to Blue: What additional costs to Blue might result from the attack?
- Purpose for Blue threat: considering all the factors above, what Red action might be deterred by this threat?

Taking the cases together, some general patterns emerge. First, most attacks on a military capability that result in a medium (or worse) degradation cause a brownout and carry a likelihood of an escalatory reaction. This includes PNT, real-time ISR, and C3. Nuclear assets carry a much higher risk. Even if the attack on the asset is non-nuclear, China could interpret this as a crossing of a nuclear red line.[38] Any dual-use asset that commingles a nuclear function with a non-nuclear function must be treated as an NC3 or NEW asset. Intelligence errors that lead to an attack on a nuclear asset are likely to result in the same response as an intentional attack, so it is imperative that targeters have high confidence about the role of their target.

Second, due to many forms of resilience, minor capability degradations are unlikely to impose much cost on Red. Commensurately, threats of minor capability degradation are unlikely to deter Red from actions in a crisis or conflict. While the equivalence of effects is unknown, minor degradations seem to be equivalent to minor trade restrictions, economic sanctions on government individuals, or diplomatic expulsions. However, they come at the risk to Blue of inviting reciprocal attacks and breaking our norms on the uses of outer space. These attacks may still carry some benefits as demonstrations of resolve or counterspace capability.

[38] C. Talmadge, "Would China Go Nuclear?: Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States" (2017); M. Stokes, G. Alvarado, E. Weinstein, and I. Easton, *China's Space and Counterspace Capabilities and Activities* (2020); A. Peczeli and B. Bahney, "The New Domains, Emerging Technologies, and Strategic Competition," in B. Roberts, ed., *Getting the Multi-Domain Challenge Right* (Livermore, CA: Center for Global Security Research, 2021), pp59-71.

Table 1: Summary of Punishing Counterspace Attacks by Target and Amount of Damage to the Capability

	Target Capability	Degradation	Cost Imposed on Red	Signals Perceived by Red	Risk to Blue	Situation/Purpose for Blue to Make Threat
Mil	PNT	Minor	Minimal, assuming resilience			Deter or punish: - Conventional posturing, maneuvering, or attacks - Precision strikes
		Medium	Degraded conventional performance	Possible Blue attack -> preemption pressure	Red reacts to preemption pressure.	
	Real-time ISR	Minor	Minimal, assuming resilience			
		Medium	Degraded situational awareness; may be localized.	Possible Blue attack -> preemption pressure	Red reacts to preemption pressure	
	Specialized ISR	Medium	Degraded/destroyed special capabilities	Pain		Counterspace demonstration
	C3	Minor	Minimal, assuming resilience			Deter or Punish: - Conventional posturing, maneuvering, or attack.
		Medium	Degraded conventional performance; may be localized.	Possible Blue attack -> preemption pressure	Red reacts to preemption pressure. NC3 is damaged / degraded.	
	NC3 / NEW	Minor	Minimal, assuming resilience	Possible Blue nuclear attack -> nuclear preemption pressure	Nuclear employment	Deter imminent Red nuclear employment
		Medium	Degraded nuclear NC3 & EW			

	Target Capability	Degradation	Cost Imposed on Red	Signals Perceived by Red	Risk to Blue	Situation/Purpose for Blue to Make Threat
Civ	PNT	Minor	Minimal, assuming resilience			Deter Red from an action or escalation by imposing pain on the population. To deter, Blue will need to make the linkage and assurance explicit.
		Medium	Economic impacts	Pain		
	ISR / Meteorology	Minor	Minimal, assuming resilience			
		Medium	Economic impacts	Pain		
	C3	Minor	Minimal, assuming resilience			
		Medium	Economic impacts	Pain		

Third, some Red infrastructure in space may present useful targets for punishment attacks. These are specialized military ISR and all civilian assets, as long as they do not have dual-use military or nuclear capabilities. In order to impose cost, the attack would have to be a medium degradation or worse. For any capability supported by a constellation, this likely means an attack that degrades several satellites amounting to a noticeable percentage of the constellation. These degradations seem to be the equivalent of major trade or economic restrictions that slow the economy. Unlike economic actions, they have the benefit of being very quick actions to take and have immediate effect. If reversible attacks are used, then the cost can be calibrated proportional to the amount of time the capability is degraded. However, the United States does not have a publicly communicated capability to perform counterspace attacks at the medium or larger scale.

Table 2: Summary of Possible Types of Punishment Attacks

Benefit to Blue	Blue Posture Required	Risk to Blue	Equivalent Cost	Actions
Demonstration or Resolve	Current		Minor economic or diplomatic	Minor degradation of mil or civ PNT, real-time ISR, C3; or specialized mil ISR
Impost Cost – Civilian	Aggressive		Major economic	Medium (or more) degradation of civ PNT, ISR, C3
Impost Cost – Military	Aggressive	Brownout likely to provoke Red escalatory response	Destruction of military infrastructure (C3, logistics)	Medium (or more) degradation of mil PNT, ISR, C3; any degrade of NC3, NEW

Implications for U.S. Posture

Current publicly known U.S. counterspace posture is quite modest, comprised of a jamming system and the suggestions (through demonstrations and tests) that some U.S. Ballistic Missile Defense (BMD) assets could pivot to counterspace missions.[39] This posture signals the capability to degrade a small number of satellites; it does not signal an intent or capability to degrade a medium or large number of satellites. Whether an attack on a small number of satellites (1-5) constitutes minor, medium, or major degradation depends on the capability being attacked. An attack on one satellite is a major degradation of a capability that is supported by one or two satellites. An attack on five satellites may only be a minor degradation of a capability that is supported by a 35-satellite constellation.

[39] T. Hitchens, "U.S. Pledges No Destructive ASAT Missile Tests, Urges International Norm" (2022); E. Heginbotham, et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017* (2015), pp233-241; and N. Strout, "This is What the Space Force Will Use to Jam Enemy Satellites" (2020).

This posture credibly supports a few classes of counterspace attacks: a minor degradation of civilian infrastructure to demonstrate U.S. resolve, or a major degradation of specialized military ISR capabilities to impose a limited cost.

A more aggressive posture with the ability to do medium damage would be needed for cost imposition on a constellation or resilient capability. This posture would include a larger number of kinetic and/or non-kinetic counterspace capabilities, fielded in geographically diverse locations to enable strikes on several satellites approximately simultaneously. The capabilities to strike at the relevant orbits (LEO, MEO, and GEO) must be accounted for; the demonstration of a LEO-strike capability does not credibly threaten MEO (where PNT is stationed) and GEO (where SATCOM is sometime stationed). The ability to use the weapons would need to be communicated through demonstrations or exercises that exhibited the training and readiness needed to execute such attacks, likely as part of joint operations with other domains. The United States currently has not publicly made any such posture known, so threats of this kind of cost imposition are not currently credible. If a country currently has this posture but is keeping its posture secret, then some degree of communication would be needed to leverage it as a deterrent threat.[40] Changing to this posture would undermine the norms and rules the United States is currently attempting to establish to prevent arms racing in space.[41] As mentioned in Table 2, using this posture to create medium degradation of civilian capabilities would be a form of cost imposition, although a cost imposed in large part on civilians. Using this posture to create medium degradations of military capabilities is an alternate form of cost imposition with the risk of incentivizing Red escalation due to the resulting brownout.

Application to Scenarios

How do considerations about how to impose cost using counterspace tools and the possible escalatory side-effects affect how these threats are wielded? The answer is dependent on the exact details of a given scenario. However, in this section, a few general United States – China scenarios are outlined. The framework is to consider a scenario, focusing on the potential action by China and the deterrent threats the United States might level at China, then to evaluate the possible change to China's cost/benefit calculus.

As noted previously, counterspace threats seem to be subtle; there does not seem to be a counterspace threat that can single-handedly deter a Chinese action. Counterspace threats seem to be more likely to have an effect as part of a larger, integrated package of coordinated threats. In that case, the question is whether the counterspace threat adds much value to the package; that is, what is the marginal contribution of the counterspace threat? Alternately stated, did the added cost of a counterspace threat change China's decision calculus, compared to the baseline case of the same threat package minus the counterspace threat? To evaluate

[40] B.R. Green and A.G. Long, "Signaling with Secrets: Evidence on Soviet Perceptions and Counterforce Developments in the Late Cold War" (2019).

[41] T. Hitchens, "U.S. Pledges No Destructive ASAT Missile Tests, Urges International Norm" (2022); F.E Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (2010), pp39-42.

this question in each scenario, Table 3 presents a package of punishment threats and an evaluation of the effectiveness of the threat. The threat is evaluated based on the cost to China relative to the stakes of the conflict and the risk to the United States in the form of misperception potential and preemption pressure. The combination of threats in the integrated threat package will vary by scenario and be calibrated to be proportional and impose sufficient cost. These threats would likely include economic sanctions, diplomatic measures, and a range of military (ground, air, sea, cyber, and space) denial threats. At the higher levels of conflict, the threat package might include nuclear punishment threats.

The subsequent rows re-evaluate that likelihood based on the addition of a counterspace threat to that package. The counterspace threats considered are the generalized threats outlined in Table 2: demonstration, civilian cost, and military cost. Note that it is possible that a counterspace threat adds some additional cost, but a substantial change is needed to change the color of a cell. The final column of the table indicates whether the additional counterspace threat provided a deterrent benefit, with acceptable additional risk, to the United States.

The coding of the cases is highly subjective and quite debatable. The coding of the likelihood of cost imposition and the possibility of side effects will be different depending on who is assigning the code, their interpretation of the confounding factors in the scenario, details of the deterrent threat, and their sense of the tipping points between costs and benefits. The author has provided this table as one example of process for visualizing these judgments.

Even in the face of all of these caveats, there is a general theme from all these cases. The crucial evaluation is the marginal difference between the baseline threat package and the packages with a counterspace threat. In most cases, the counterspace threat doesn't change China's calculus in the United States' favor. The best that adding a counterspace threat can do for the United States is to not make the situation worse. In many cases below the conventional threshold, adding a counterspace threat beyond a minor attack for the demonstration of capability and resolve is disproportionate and adds escalation risk due to the brownout effect. A more detailed coding of this table—by careful study, modeling, or SME elicitations—seems unlikely to change this outcome. Said another way, although the coding of these scenarios is a subjective judgement call and subject to debate, this paper argues that it will be difficult to find a case where the coding of a counterspace deterrent threat is advantageous to the United States relative to the baseline threat package.

Table 3: Counterspace Threats as Part of a Package of Non-Conventional Integrated Deterrent Threats.

United States Wants to Deter Action by China…	United States Threatens…	Is cost on China potentially adequate to deter?	Misperception potential and/or preemption pressure	Change in United States' cost/benefit due to counterspace threat
Economic manipulation (currency, IP theft, trade issues)	Cyberattacks, economic sanctions			
	Above + Counterspace (CS) Demonstration	Disproportionate	Dual-use infrastructure?	
	Above + CS Civilian Cost	Disproportionate	Dual-use infrastructure?	
	Above + CS Mil Cost	Disproportionate		
Minor attacks on U.S. space or cyber infrastructure (during a militarized crisis)	Cyberattacks, economic sanctions			
	Above + CS Demonstration	Communicate capability; retaliate in kind	Dual-use infrastructure?	
	Above + CS Civilian Cost	Communicate capability; retaliate in kind	Dual-use infrastructure?	
	Above + CS Mil Cost	Disproportionate		
Medium attacks on U.S. space or cyber infrastructure (during a militarized crisis)	Cyberattacks, economic sanctions			
	Above + CS Demonstration	Communicate capability; retaliate in kind	Dual-use infrastructure?	
	Above + CS Civilian Cost	Communicate capability; retaliate in kind	Dual-use infrastructure?	
	Above + Mil Cost	Disproportionate		

United States Wants to Deter Action by China…	United States Threatens…	Is cost on China potentially adequate to deter?	Misperception potential and/or preemption pressure	Change in United States' cost/benefit due to counterspace threat
Blockade of Taiwan	Economic sanctions, cyberattacks, military intervention			
	Above + CS Demonstration	Doesn't add cost relative to stakes[42]	Dual-use infrastructure?	
	Above + CS Civilian Cost	Doesn't add cost relative to stakes	Dual-use infrastructure?	
	Above + CS Mil Cost	Doesn't add cost relative to stakes		
Attack on Taiwan	Economic sanctions, cyberattacks, military intervention.	China's stakes are high.		
	Above + CS Demonstration	Doesn't add cost relative to stakes	Military situation is already critical	
	Above + CS Civilian Cost	Doesn't add cost relative to stakes	Military situation is already critical	
	Above + CS Mil Cost	Doesn't add cost relative to stakes	Military situation is already critical	
Conventional Escalation, as attack on Taiwan stalls.	Economic sanctions, cyberattacks, military intervention and retaliation.	China's stakes are high	Military situation is already critical	

[42] E. Colby and D. Ochmanek, "How the United States Could Lose a Great-Power War," *Foreign Policy* (October 29, 2019), https://foreignpolicy.com/2019/10/29/united-states-china-russia-great-power-war/, accessed April 2022.

United States Wants to Deter Action by China…	United States Threatens…	Is cost on China potentially adequate to deter?	Misperception potential and/or preemption pressure	Change in United States' cost/benefit due to counterspace threat
	Above + CS Demonstration	Doesn't add cost relative to stakes	Military situation is already critical	
	Above + CS Civilian Cost	Doesn't add cost relative to stakes	Military situation is already critical	
	Above + Mil Cost	Doesn't add cost relative to stakes.	Military situation is already critical	
Nuclear Escalation, as attack on Taiwan stalls.	Economic sanctions, cyberattacks, military intervention and retaliation.	China's stakes are high	Military situation is already critical	
	Above + CS Demonstration	Doesn't add cost relative to stakes	Military situation is already critical	
	Above + CS Civilian Cost	Doesn't add cost relative to stakes	Military situation is already critical; dual use?	
	Above + CS Mil Cost	Doesn't add cost relative to stakes	Military situation is already critical	

Color Key: Is the scenario a net positive for the United States? Dark green, very positive; light green, somewhat positive; yellow, neither positive nor negative; orange, somewhat negative; red, highly negative. Fifth column: what is the net gain to Blue by adding the counterspace attack into the baseline threat package? Green, positive gain; white, no gain or loss; red, negative effect (high risk and low additional benefit).

Conclusion

Integrated strategic deterrence relies on bringing together a network of national capabilities across military and civilian domains to achieve the country's goals. For this to be effective, decisionmakers must understand how these diverse capabilities can be applied and what results can be obtained. As part of that understanding, this paper explores the role of counterspace assets to level deterrent threats at another country. This is separate from counterspace assets' role in deterrence by denial, which flows from their effectiveness for denial. Can counterspace threats against Red's space infrastructure be used to deter Red actions beyond the space domain? If so, then counterspace threats may play a role in cross-domain, multi-domain, and integrated deterrence.

Deterrence functions in the context of an anticipated action by Red. Deterrence by punishment works on Red's cost/benefit evaluation (which may be more notional than explicit) by asserting that Blue will deliberately impose an additional cost on Red in the aftermath of Red's action. For the assertion to have a chance of affecting Red, Blue must have the capability, Blue must communicate the capability and intention to Red, and Red must find the threat credible.

Space infrastructure, military and civilian, is generally information infrastructure. National and commercial satellites (and their supporting ground systems) are used for communications, PNT, and ISR. Degrading satellites is therefore degrading information capabilities of some kind, and the cost imposed on the target country is an information brownout—effectively the loss of this information. However, the severity of the degradation in information capability depends on a few factors, including: Can Red get the information other ways, whether by terrestrial networks or other satellites in the constellation? What is the geospatial and temporal expanse of the information loss? Can Red do without the information? And, crucially, as the sudden loss of the information adds to the "fog of war" and communicates an intent to attack, what is the likelihood of accidental or inadvertent escalation?

The evaluation presented in this paper suggests that counterspace attacks are not a strong contributor to the network of military tools decisionmakers have for deterrence by threats of punishment. Small attacks (1-2 satellites) may signal resolve, but don't impose much cost. The United States doesn't communicate the posture for large, cost-imposing attacks. If it did, large attacks on civilian infrastructure in space is the best opportunity for cost imposition; such attacks may impose costs similar to economic sanctions or blockades but run counter to U.S. norms. Crucially, large attacks on military infrastructure in space create an information brownout that in turn creates conditions for misperception and escalation. When tailoring an integrated package of punishment threats in a specific situation, decisionmakers are likely to find that the counterspace threat rarely adds to the threat, and frequently makes the situation worse due to undesired information brownout side effects.

Counterspace capabilities do play a role in joint operations or the denial of Red military aims. And, as part of a credible military denial capability, they further play a role in deterrence by denial.

Acknowledgements

The author is grateful to Ben Bahney, Jonathan Pearl, Michael Markey, Brandon Williams, Brian Radzinsky, Asmeret Asghedom, Kristine Wong, and Brad Roberts for their suggestions, guidance, and mentoring.

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-MI-845664