April | 2018

NSI Concept Paper…….

Space Deterrence: The Vulnerability-Credibility Tradeoff in Space Domain Deterrence Stability

Prepared for
Strategic Multi-Layer Assessment
Contested Space Operations

Ali Jafri, NSI
ajafri@NSIteam.com

John A. Stevenson, Ph.D., NSI
jstevenson@NSIteam.com

Citation: Jafri, A. & Stevenson, J. (2018). *NSI Concept Paper, Space Deterrence: The Vulnerability-Credibility Tradeoff in Space Domain Deterrence Stability,*. Arlington, VA: Strategic Multi-layer Assessment (SMA). Retrieved from http://nsiteam.com/sma-publications

Introduction

Many deterrence theorists posit that the application of deterrence principles in the space domain will engender different results than their applications in other domains. These differences come in part from the peculiar qualities of the physical environment of space, and from the risk that states incur from an increasing reliance on space's role in multi-domain strategies. These risks have created a consensus that space deterrence stability will be enhanced by increasing the resilience and protection of space systems. Most commonly accepted recommendations for space deterrence stability are actions that, in aggregate, aim to reduce risk, and thereby, inadvertently reduce the credibility of response.

However, we argue that unmitigated risks of dependence on the space domain enhances the credibility of the most space-dependent nations; the reliance on the domain creates a credible threat that a state whose space assets are intentionally degraded or destroy will commit to a firm, not necessarily proportional response. The limited situational awareness of the domain is informed by an inability for clear attribution; the attribution problem is a domain characteristic and is not necessarily any more of a problem for our argument than a problem of space and cyber deterrence in general. Assuming that the deterring country can attribute an intentional space attack to an adversary, then it could counter with a firm, yet not necessarily proportional responses. Such response allows the deterring country to manipulate the calculated risk an adversary would entertain to achieve terrestrial gains through limited, temporary or reversible attacks on space assets. Attacks in space are most likely serving a terrestrial objective that may not take very long to achieve. The implication of this means that space-dependent states need to communicate that when attacks are attributed, the attackers understand that a firm response to the space attack will occur decoupled from the time horizons and objectives of other objectives and other domains.

The Concept Paper is organized as follows. After distinguishing between two types of warfighting uses—*indirect* assistance to war fighting capabilities and *direct* basing of weapons of space, we specify two corresponding types of deterrence, referred to herein as Type 1 and Type 2 deterrence. Type 1 deterrence concerns the defense of space assets which indirectly assist warfighting capabilities. Type 2 deterrence, on the other hand, concerns the prevention of the basing of weapons in space. We then hone in on Type 1 deterrence; we argue there exists a *vulnerability-credibility tradeoff* due to peculiar characteristics of the space domain and how the United States leverages space to enhance other elements of national power. The vulnerability-credibility tradeoff is a critical insight for national security space operators to understand because of divergence from classic deterrence models. Specifically, in classic deterrence having less capability to mitigate a vulnerability never makes an actor better off in maintaining a status quo.[1] In space however, we conclude the opposite: remaining reliant or dependent upon vulnerable space

[1] Although we will not explore this aspect of the argument here due to space constraints, many theorists of coercion would say that growing vulnerabilities not only lessen deterrence stability, but they also open the target to acts of compellence and blackmail.

capabilities makes our commitment to Type 1 deterrence more credible, lessening incentives for (kinetic or other forms of) aggression in crisis and conflict.

How Does the United States Use Space?

The two superpowers first placed assets into the space domain space system assets during the Cold War. Between 1957 and 1990, 93% of all satellites launched into space were attributable to either the United States or the Soviet Union (Harrison, Cooper, Johnson & Roberts, 2017). Military satellites once purposed primarily for nuclear missions are now also used routinely for conventional and sub-conventional maneuver (Harrison et al., 2017). Over time, these space assets were re-purposed into helping the United States extend its advantage in multiple domains. Dr. Cassandra Steer of Women in International Security-Canada summarized the current reality succinctly, "space is…utilized in a unique way compared to all other domains" because it (as well as cyber) is an enabler to other domains, without which those domains could not function optimally (Pagano, 2018). Representatives of ViaSat, a leading space company, underscored the United States' increased dependence on space noting that:

> Space systems that deliver communications, Earth observation, position/navigation/timing, missile warning, weather, etc. do not exist exclusively in space. Their delivery platforms, or infrastructure, exist in all domains including land, sea, air, space, and cyber[2] (ViaSat, personal communication, January 25, 2018).

"Space assets", which we use interchangeably with "space capabilities", refer to more than just the satellites in orbit. Without data uplinks to fly and control the satellites and data downlinks to transfer information from space, satellites are of limited use; moreover, much of the data coming from space requires a significant amount of processing to be usable by consumers. Unless otherwise noted, therefore, "space asset" refers to the entire system comprising the physical satellite, data uplink and downlink systems, ground stations, and information processing and distribution. Collectively, space systems encompass a wide breadth of capabilities, including, but not limited positioning, timing, and timing (PNT) satellites. These systems, which also include GPS satellites, are able to determine their location in space because of communication infrastructure that links them to terrestrial counterparts; they provide information to military, civilian, and commercial users. PNT satellites' broad utility is illustrative of the larger dependency of the United States on space systems. The National Academy of Sciences, in a 2016 report write:

[2] See the NSI Space ViTTa® Q17 report conducted for SMA on multi-domain conflicts: Multi-Domain Conflicts: Is US Success Contingent on Dominance in Every Domain? at http://nsiteam.com/sma-publications.

> …space systems are a critical component of the national security services we now take for granted: Communication satellites, space-based imagery, positioning, navigation, and timing (PNT), and signals intelligence provide navigation and mission awareness for U.S. and allied military personnel on the ground, in the air, and at sea. They are also the backbone of the blue-force tracking that has greatly reduced casualties from friendly fire, and they underpin the cost- and collateral damage-reducing precision targeting and strike that Americans now expect of kinetic military operations.[3]

While the United States' multi-domain dependence on functioning space assets has deepened, an array of other state and non-state actors, some potentially hostile to the United States, accelerated the rate at which they have added assets to the space domain (Stevenson and Popp, 2018). After 1991, through 2016, only 57% of new satellites and 61% of launches are attributable to Russia and the United States (Harrison et al., 2017). Concerning government-launched satellites, both the United States and Russia's relative share of satellites and launches continues to steadily decrease; since 2014, other countries, such as China, Japan, Europe, and India, have seized the lead in satellites and launch (Harrison et al., 2017).

There are two dimensions to how space assets magnify the United States' advantages in other domains:

- **Indirect Assistance of Warfighting Capabilities**: Indirect magnification of war fighting capabilities stem from those assets that facilitate communications, Earth observation, position/navigation/timing (PNT), and missile detection. The indirect dimension is about assistance and connection.

- **Direct Warfighting Capabilities**: Direct magnification of war fighting domain comes from those assets that can directly harm infrastructure or forces in any domain. Direct dimensions include deployed anti-satellite technology, jamming signals, etc.

With respect to the indirect assistance of warfighting capabilities, space assets are characterized as providing three broad categories of information services: communications; PNT; and observation and surveillance. Though indirect, were any of these services interrupted, the United States would have limited command and control (C2) over its nuclear forces, and restricted early warning systems. Without PNT, much of our modern way of maneuver would become unwieldy: terrestrial forces would find navigation more difficult, surgical attacks harder to perform, and there would be a higher risk of friendly fire between allied units due to communications losses.

[3] See the NSI Space ViTTa® Q17 report conducted for SMA on multi-domain conflicts: Multi-Domain Conflicts: Is US Success Contingent on Dominance in Every Domain? at http://nsiteam.com/sma-publications.

The Two Types of Space Deterrence

The *classic model of deterrence* involves a deterring actor seeking to credibly threaten to impose negative consequences on a target if that target takes an action to change the status quo.[4] The elements of successful, stable deterrence therefore are:

- The actor seeking to deter establishes a status quo and can credibly threaten a target with negative consequences if the target takes a certain action or violates a prohibition.
- The deterring actor also credibly assures its target that no negative consequences will follow if compliance is achieved.
- The targeted actor refrains from taking the prohibited specific activities.

The proliferation of actors, interests, capabilities, and objectives in the domain has clouded the environment in such a way that it would be unrecognizable to Cold War strategists: The distinguishing features of the space domain corrodes the foundations upon which stable and successful deterrence in the classic model rests, namely threat credibility, and clarity in assurances (Harrison et al., 2017). Although most space-faring nations have the capability to pose credible threats in many domains, inclusive of space and cyber, the core problems of proper attribution and the willingness to execute threats in cases of violation remain (Danilov, 2001). These commitment problems mean that we would be wise to avoid "unerring straight-line extrapolation" from other domains to space (Astorino-Courtois, 2018). In other words, the principles of deterrence as classically applied require careful tailoring for use in the space domain to safeguard the United States and its allies.

Multi-domain dependence on space capabilities creates critical strategic vulnerabilities which adversaries could potentially exploit to intentionally disrupt information services. Adversaries can target any aspect of space capabiltiies, whether those assets are based in space or terrestrially. What is being deterred in

[4] The classic deterrence literature is vast. Central pieces include: Bernard Brodie, "The Anatomy of Deterrence," *World Politics* Vol. 11, No. 2 (1959); Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960); Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, N.J.: Princeton University Press, 1961); Bruce Russett, "The Calculus of Deterrence," *Journal of Conflict Resolution* Vol. 7, No. 2 (1963); Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Stephen Maxwell, *Rationality in Deterrence*, *Adelphi Papers 50* (London: IISS, 1968); Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Robert Jervis, "Deterrence Theory Revisited," *World Politics* Vol. 31, No. 2 (1979); John J. Mearsheimer, *Conventional Deterrence* (Ithaca, N.Y.: Cornell University Press, 1983); Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989).

space deterrence are *intentional attacks against space capabilities, regardless of physical location*.[5] Space deterrence theorists universally agree with safeguarding space capabilities from intentional targeting as being the foundation of what space deterrence distinctly is pre-occupied with. For example, Michael Krepon defined space deterrence as the "deterring harmful actions by whatever means against national assets in space and assets that support space operations (Krepon, 2013).

Deterrence theorists have already categorized the range of types of attacks against space capabilities that space deterrence seeks to prevent. These attack types range from demonstrably kinetic to cyberattacks, and are described in Table 1.[6] The enclosed table illustrates a range of possible attacks on space systems, along with several particular characteristics of that attack type that would affect the effectiveness of space deterrence.

- **Attribution**: This characteristic describes the difficulty of determining the intentionality of the attack.
- **Irreversibility**: The characteristic depicts how permanent the damage from the attack type would be on the space capability.
- **Attacker Damage Assessment**: This characteristic captures whether adversarial actors would have confirmation that their attack successfully impeded some functioning of the space capability.

Table 1: Type Attacks to Be Deterred

	Kinetic	Electronic	Cyber
Attribution	Variable	Modest	Limited/uncertain
Irreversibility	Irreversible	Fully reversible	Variable
Attacker Damage Assessment	Near real-time confirmation of success	Limited or no confirmation of success	Near real-time confirmation of success

[5] Unintentional interference may happen, simply from the technical challenge of operating machinery in space or the way waves and signals reach satellites. This paper's argument does not apply to interference that arises from current limitations in engineering or the asset degradation that stems from the harsh physical environment of space.

[6] Adapted from Harrison et al., 2017.

Table 1 has three categories of attack types against space capabilities, each of of which presents particular challenges for deterrence theory. Kinetic attacks are all actions taken to compromise the physical aspects of the space capability. After kinetic attacks, the specific physical pieces of the space asset no longer function, and in some cases, become space debris. These include, as examples, impact (kinetic kill), proximity explosion, electro-magnetic threats, as well as EMP, laser, microwaves and neutron beams. Electronic attacks are those attacks which impede the functioning of a space asset through transitory effects, and, as such, do not create space debris and may delay attribution. Examples of electronic attacks comprise: harassing, transitory jamming or dazzling interference. Cyber attacks target the information services aspects of space capabilities, as well as the operators' control over the asset.

Each of the three charateristics is an evaluative measure of space deterrence stability. By manipulating the risk that a space asset is not irreversibily destroyed, the risk of attribution of intent, or the adversaries awareness of the damage, these categories depict the decision calculus that both the adversary and the deterring actors would face in choose to attack and respond, respectively. Limiting attribution, reversibility, and increasing damage awareness, in theory, increases the benefits and reduces the cost of adversarial action. Similarly, limiting attribution, reversibility, and increasing damage awareness, in theory, can reduce the credibility of the deterrer to respond to the attack.

In order to achieve the goal of a strategic environment in which intentional attacks against space capabilities does *not* occur, the applications of space deterrence would fall into two distinct types.

- Type 1 Space Deterrence: This type of space deterrence has as its strategic goal space asset infrastructure security. This includes the prevention of spillover of conflicts in other domains into space (multi-domain war) that target space capabilities.
- Type 2 Space Deterrence: The second type of deterrence is the prevention of the weaponization and the basing of multi-domain weapons in space.

Col. Timothy Cullen of the United States Air Force reasoned that considering both types of deterrence is necessary to achieve the goals of robust space deterrence. Cullen argues that for space to remain relatively peaceful:

> Countries, to include the US, [must] choose not to deploy weapons—or unambiguous military targets—in space. In parallel, the US government must ensure its military and its

> allied forces are sufficiently redundant to employ lethal and decisive force independent of space assets, if required.[7]

We agree with Cullen, and the wider space deterrence community, that the challenge of Type 2 is a straightforward application of deterrence principles: The status quo is no actor possesses a weapon that is directly based in space. Type 2 Deterrence is seeking to maintain that status quo.

We disagree with Cullen that building redundancy to limit the effectiveness of an attack will aid in the pursuit of successful, stable space deterrence. Type 1 attacks may occur a variety of reasons. Space deterrence does not include the successful deterrence of the terrestrial issues that may be driving conflict between adversaries. For example, space deterrence is successful if neither the United States and Russia were to target each other's space assets to achieve a situational advantage in Crimea or in retaliation for Russia's interference in the United States' 2016 presidential election, irrespective of whether those underlying 'terrestrial' conflicts get resolved or even intensifies. (Stevenson, 2018).

Denial *is* Just a River in Egypt: Why Type 1 Space Deterrence Requires Punishment to Be a Credible Deterrent

Some space systems have components that reside within other earth-based domains. An adversary's conventional goals may lead to the targeting of space assets to disrupt the indirect support space assets grant our conventional forces. Importantly,

> a network infrastructure loss in any of these domains equates to a loss in providing service or delivery to their customers that operate in the land, sea, air, space, [and cyber] domains. The inability to defend and protect systems in all domains leads to loss of service or operational capability in the operational domains of land, sea, air, space, [and cyber].[8]

Other space deterrence theorists typically offer solutions to this problem of Type 1 space deterrence similar to those proferred by Col. Collen. These solutions emphasize building redundant information services capabilities in case of an attack on our space assets. This approach, however, is a fallback plan: In seeking to make an attack on space assets less useful, this approach hopes that it is also deterring the attack in the first place. Space systems' resilience and redundancy is presented as option that creates

[7] See the NSI Space ViTTa® Q10 report conducted for SMA on the effects of government and commerical investment and commitment on space security and the likelihood of kinetic military action at http://nsiteam.com/sma-publications.

[8] See the NSI Space ViTTa® Q17 report conducted for SMA on multi-domain conflicts: Multi-Domain Conflicts: Is US Success Contingent on Dominance in Every Domain? at http://nsiteam.com/sma-publications.

post-attack capability survivability, and through survivability, a credible deterrence of denial that safeguards the means of retaliation.

Yet, this deterrence of denial does not directly confront the incentives of adversaries to intentionally target space assets to achieve aims in other domains; approaching Type 2 space deterrence through a denial framework loses sight of the necessary component of successful, stable deterrence: the defender's credibility of commitment that aggression will be responded to—that is, a deterrence of punishment.

Achieving Type 2 space deterrence by punishment requires that the US demonstrates the political will to inflict costs on adversaries that intentionally target space assets. The United States gains the credible resolve to respond to attacks from its extreme multi-domain dependence on functioning space systems. All space deterrence theorists agree that the United States simply cannot afford any loss or disruption of its space cabilities. If all adversaries know that the United States is aware of this vulnerability, then the United States can credibly threaten to respond to any intentional attack that results in a space systems' loss or disruption.

In other words, Type 2 space deterrence exhibits a heretofore unnoticed *vulnerability-credibility tradeoff* that is not present in classic deterrence and that space deterrence by denial exacerbates. While limiting resilience and redundancy would increase the United States' capabilities to achieve domain in each domain, as it is a vulnerability in the space domain, it is a boon for space deterrence in generating credibility of resolve. Steps taken to mitigate this vulnerability would limit the credibility of resolve to maintain the status quo as depicted in Figure 1.

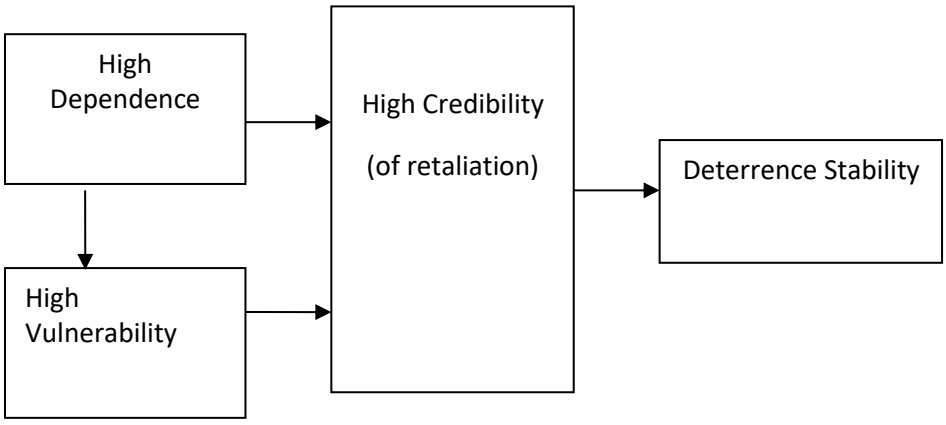

Figure 1: Pathways to Space Deterrence Instability

The threshold for an attributable attack which would produce a credible response is low. Because of the multi-domain dependence on space assets and capabilities, any attributable attack would likely elicit a response from the object actor. However, it is important to understand that the lack of a response on an intentional degradation of space capabilities by an adverse actor does not represent deterrence failure. It is instead due to specific domain charactersitcs that cloud the environment.

Conclusion: Implications of the Tradeoff

Space deterrence is affected by several distinct characteristics of the space domain.

1. Space is remote: The distance and speed at which satellites operate makes them difficult to inspect, track, or assess damage from attacks. Conflict could be conducted remotely by both the attacker and defender with little to no direct risk of human casualties.
2. The natural environment is dangerous: There are many natural threats that can mask the effects of deliberate attacks. Naturally occurring threats in space include meteors and fragments, as well as sun flares and other inclement space weather that can damage or destroy the satellite itself or the electronics riding on it. Ground- or air-based components of space systems are also subject to natural causes of service interruption and damage.
3. There are no distinct borders: Satellites cross over the territories of other nations, and no nation has control of the orbital space above or adjacent to its territory.
4. There has been no major conflict: Few examples of escalation and de-escalation exist as customary knowledge within the domain.
5. Attribution is difficult: Because of the inherent fog of the domain, i.e. the inability to clearly attribute attacks, space actors are able to maintain some level of plausible deniability when it comes to response to attacks on space assets.

The current U.S. approach to space has re-focused on cislunar space and manned space exploration (Harrison and Johnson, 2017). The 2017 U.S. National Security Strategy declares that the "United States considers unfettered access to, and freedom to operate in space to be a vital interest," and in protection of that interest, 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". Currently, the United States will remain dependent on space for key aspects of US economic, social and military power. We believe that in light of the vulnerability-credibility tradeoff, the flexible, firm response suggested in current United States space policy is well-suited to deterrence in space.

References

Astotino-Courtois, A. (January 2018). How Should Space Feature in US Deterrence Strategy. Retrieved from http://nsiteam.com/space-feature-deterrence-strategy/.

Cheng, D., Garretson, P., Polpeter, K., and Wright, N. (2018). "China's Perspectives on Space Deterrence and Escalation." *Strategic Multilayer Assessment Space Panel Discussion*. For access to the audio recording of this event, please contact Nicole Peterson at NPeterson@NSIteam.com.

Danilov, V. (June 2001) "The Sources of Threat Credibility in Extended Deterrence" in *The Journal of Conflict Resolution*. 45: 3, pp. 341-369. Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.291&rep=rep1&type=pdf.

Harrison, R., Jackson, D., & Shackleford, C. (2009). *Space Deterrence: The Delicate Balance of Risk*. In Space and Defense, Volume 3, Issue 1.

Harrison, T., Cooper, Z., Johnson, K., Roberts, T. (2017). Escalation and Deterrence in the Second Space Age. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171109_Harrison_EscalationDeterrenceSecondSpaceAge.pdf?pkaq8A3h5rRj8zkOrL2bDpUa4MtjERPa.

Harrison, T., & Johnson, K., (2017). Back to the Moon? Understanding Trump's Space Policy Directive 1. Retrieved from https://www.csis.org/analysis/back-moon-understanding-trumps-space-policy-directive-1.

Hendrix, J., Routh, A. (2017). A Space Policy for the Trump Administration. Retrieved from https://s3.amazonaws.com/files.cnas.org/documents/Space-Policy-for-the-Trump-Administration.pdf?mtime=20171023110127.

Huth, P. K. (1999). Deterrence and international conflict: Empirical findings and theoretical debates. Annual Review of Political Science, 2(1), 25-48.

Krepon, M. "Space and Nuclear Deterrence," quoted in Michael Krepon and Julia Thomas, eds., Anti-Satellite Weapons, Deterrence and Sino-American Space Relations, Washington, D.C.: Stimson Center: 2013.

Kroenig, M. (2013). Nuclear Superiority and the Balance of Resolve: Explaining Nuclear Crisis Outcomes. International Organization, 67, pp 141-171 doi:10.1017/S0020818312000367.

Libicki, M. (2009). Cyberdeterrence and Cyberwar. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Lupovici, A. (2010). The emerging fourth wave of deterrence theory—Toward a new research agenda. International Studies Quarterly, 54(3), 705-732.

National Academies of Sciences, Engineering, and Medicine. 2016. *National Security Space Defense and Protection: Public Report*. Washington, DC: The National Academies Press. Retrieved from https://doi.org/10.17226/23594.

National Aeronautics and Space Administration. (2017). New Space Policy Directive Calls for Human Expansion Across Solar System [Press Release]. Retrieved from https://www.nasa.gov/press-release/new-space-policy-directive-calls-for-human-expansion-across-solar-system.

National Security Strategy of the United States of America, 2017. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12 18-2017-0905.pdf.

National Space Policy of the United States of America, 2010. Retrieved from https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf.

Pagano, S. (2018). Is US Success Contingent on Dominance in Every Domain? Retrieved from http://nsiteam.com/is-us-success-contingent-on-dominance-in-every-domain/.

Popp, G. (2018). Strategic Risk in the Space Domain. Retrieved from http://nsiteam.com/strategic-risk-in-the-space-domain/.

Schelling, T. (1966). *Arms and Influence*. Yale University Press.

Sechser, T., Fuhrmann, M. (2013). Crisis Bargaining and Nuclear Blackmail. International Organization, 67, pp 173-195 doi:10.1017/ S0020818312000392.

Stevenson, J. (2017). *NSI Concept Paper, Gray Zone Deterrence: What It Is and How (Not) to Do It.* Arlington, VA: Strategic Multi-layer Assessment (SMA). Retrieved from http://nsiteam.com/social/wp-content/uploads/2017/06/CP3_Deterrence_Final.pdf.

Stevenson, J. & Popp, G. (2018). National Security Implications of Space Launch Innovations. Retrieved from http://nsiteam.com/security-implications-of-commercial-launch-services/.

The White House, Office of the Press Secretary. (December 11, 2017). *President Donald J. Trump Will Make America a Leader in Space Exploration Again* [Fact Sheet]. Retrieved from https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-will-make-america-leader-space-exploration/.

The White House, Office of the President. (December 11, 2017). *Presidential Memorandum on Reinvigorating America's Human Space Exploration Program* [Presidential Memorandum]. Retrieved from https://www.whitehouse.gov/presidential-actions/presidential-memorandum-reinvigorating-americas-human-space-exploration-program/.

U.S. Joint Chiefs of Staff. (August 9, 2002). Joint Doctrine for Space Operations, Joint Publication 3-14. Retrieved from http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf.

Zagare, F. C. (2004). Reconciling rationality with deterrence: A re-examination of the logical foundations of deterrence theory. Journal of Theoretical Politics, 16(2), 107-141.