AIR WAR COLLEGE

AIR UNIVERSITY

ACHIEVING ALLIANCE SPACE DETERRENCE:

A PROPOSAL FOR NATO "SPACE DEFENSE"

By

Eugene C. Richter, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

SSP Advisor: Col Galen K. Ojala

Space Chair to Air University

22 Mar, 2024

Maxwell AFB AL

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col Eugene C. Richter is a United States Air Force Foreign Area Officer and candidate for Master of Strategic Studies at Air War College, Air University (Maxwell AFB, AL). Gene's career spans 24 years and includes assignments supporting all Geographic Combatant Commands and Headquarters Air Force. He currently serves as head of Security Cooperation and IMA to the Director, International Affairs at Space Operations Command, United States Space Force.

Abstract

Reflecting a new era of accelerating counterspace threats, this paper intends to provide recommendations for measures NATO could adopt to strengthen its space deterrence posture. It begins with a review of deterrence theory, emphasizing how space deterrence derives and diverges from classical deterrence concepts. It then explores space deterrence "in practice" for an individual spacefaring nation, identifying the requirements for such deterrence. It then offers an overview of the NATO space enterprise and concludes by adapting space deterrence requirements to the alliance. The paper concludes with recommendations for strengthening NATO space deterrence including: 1) NATO should embrace "Space Defense" as a component alliance deterrence and defense; 2) NATO should develop strategy and doctrine to implement a mixed space deterrence strategy that includes space defense and resilience measures; 3) NATO should integrate space forces into its ready forces (e.g. Multinational Battlegroups and the Alliance Response Force); and 4) NATO should integrate the full spectrum of counterspace threats into exercises at all echelons from field unit to NATO Headquarters.

Introduction

Russia's surprise direct-assent anti-satellite demonstration in December 2021 scattered a debris field of more than 1,500 trackable objects. The incident necessitated multiple orbit adjustments to the International Space Station and created a life-threatening minefield of possibly hundreds of thousands of non-trackable objects that space-faring nations will be dealing with for decades to come.[1] Just months later during its full-scale invasion of Ukraine, Russia jammed the regional ViaSat commercial satellite network, virtually eliminating Ukraine's military command and control along with satellite communication service to tens of thousands of European customers.[2]

China has placed into orbit various hunter-killer spacecraft designed to disable or destroy on-orbit satellites. China has also tested high powered land-based anti-satellite laser and microwave systems and has likely placed counterspace kinetic weapons into orbit.[3] With the barriers for entry into the space domain collapsing by the day, and it is only a matter of time before other state and non-state actors will be equally capable of holding space-based assets at risk.

While space-faring nations have alerted to this reality and begun mitigating efforts, NATO *as an alliance* came to the realization rather late. NATO did not recognize space as an operational domain until December 2019, and only in 2022 published its first space policy. Though still in its formative stage, the alliance has taken important steps to bring its capabilities

[1] "Competing in Space," 2d edition. National Space Intelligence Center, Air Force Public Affairs, 2023, https://www.spoc.spaceforce.mil/Portals/4/Images/2_Space_Slicky_11x17_Web_View_reduced.pdf.
[2] "Case Study: Viasat" Cyber Peace Institute, accessed Dec 10, 2023, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.
[3] "Competing in Space"

in line with its ambition. It established the NATO Space Center in Ramstein, Germany in October 2020, which has provided daily space support to NATO operations since early 2023. NATO also established a Center of Excellence in Toulouse, France in July 2023.[4] With the ever increasing threats to Alliance space operations, NATO must move faster to adapt its deterrence and defense mission to incorporate threats in, from, and to space. This paper aims to support that effort by identifying essential capabilities and measures NATO should consider to achieve effective space deterrence.

The paper consists of three parts. Part One: *Defining Space Deterrence*, provides an overview of contemporary deterrence theory and concepts as it relates to the emerging field of space deterrence. Part Two: *Achieving Space Deterrence,* draws from existing literature to explore what effective space deterrence looks like and what is required to achieve it. Part Three: *NATO Space Deterrence*, applies the concepts from the first two parts to the NATO space enterprise.

The paper is intended for an audience with a basic familiarity with space concepts but does not venture beyond doctrine-level discussions of space capabilities, technical concepts, or orbital science.

[4] "Lift Off: NATO Launches New Space Center of Excellence," NATO ACT, accessed March 24, 2022, 2024, https://www.act.nato.int/article/space-newest-coe/

Part 1. Defining Space Deterrence

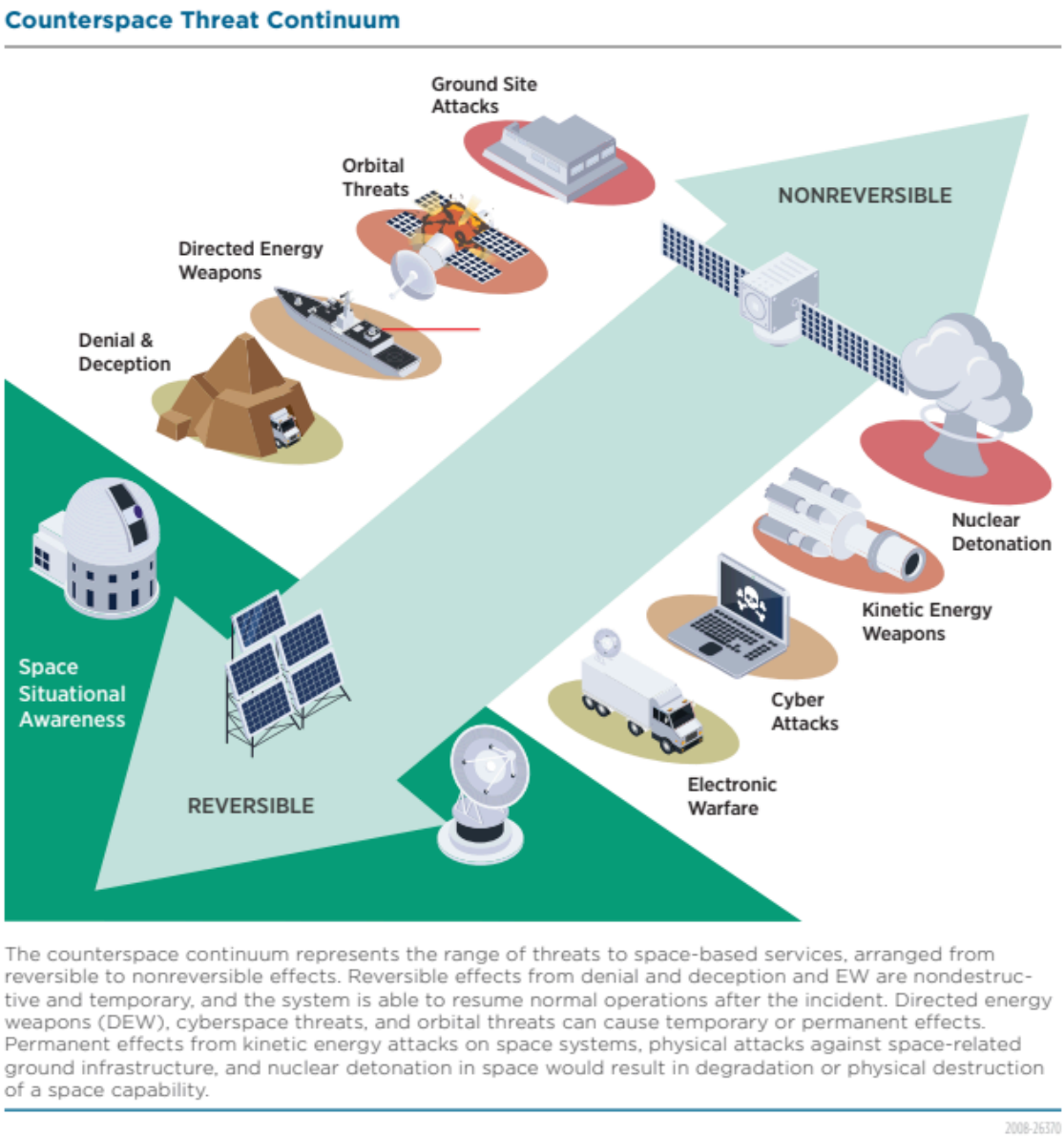
Space deterrence, sometimes referred to as "deterrence for space" or "deterrence in space operations,"[5] is the application of deterrence concepts to the military space domain. The space deterrence literature diverges from classical deterrence theory in that its focus is on the object being deterred, rather than the means of deterrence. In other words, classical deterrence focuses on the means with which a defender threatens an aggressor with retaliation, i.e. nuclear or conventional *means*. Space deterrence focuses on how to deter attacks on capabilities within the space *domain*, not necessarily on the use of space-enabled *means* to deter aggression. Space capabilities may constitute some or all of the deterrent means of space deterrence strategies, but they are not the focus of the strategy.

Space deterrence concerns how to dissuade an adversary from taking hostile measures to deny, degrade, disrupt, or destroy one's space assets and capabilities. These "counterspace" threats can range from temporary actions such as jamming a spacecraft's link component, to the complete destruction of an on-orbit space asset.

Counterspace threats present along a continuum from reversible to irreversible (the degradation or destruction is permanent) and are either kinetic or non-kinetic. Non-kinetic threats be can further broken down into active, such as electromagnetic "jamming" or cyberattacks, or passive, such as masking or concealment of space capabilities. The figure below provides a

[5] Flanagan, Stephen J., Nicholas Martin, Alexis A. Blanc, and Nathan Beauchamp-Mustafaga, A Framework of Deterrence in Space Operations. Santa Monica, CA: RAND Corporation, 2023. https://www.rand.org/pubs/research_reports/RRA820-1.html.

graphic depiction of the counterspace threat continuum from non-kinetic and reversible to kinetic and non-reversible:[6]



[6] "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion" Defense Intelligence Agency, 2022, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

Adversaries come to the competition with a wide range of counterspace capabilities, strategies, and hostile intent. China and Russia pose the greatest counterspace threats to all three segments of space operations (ground, link, space), but other nations such as North Korea and Iran continue to develop and deploy their own counterspace capabilities.[7] The most dangerous threats include space nuclear detonation (NUDET) and direct assent anti-satellite (ASAT) missile attack, both of which would have profound and enduring consequences.[8] Countries with more space-based assets may be more risk-averse in pursuing kinetic strategies, while others might see destruction of on-orbit assets as their best option to pursue when confronting a major space power in terrestrial conflict. Other actors may be highly skilled in cyberwarfare and will focus their efforts on that domain. Effective space deterrence thus requires a defending nation, or an alliance such as NATO, to deter aggression throughout the counterspace threat continuum.

Cyber Parallels

Many on-orbit space capabilities are inherently cyber-centric, in that they depend on large data flows over electromagnetic communications networks. For this reason, the domains share similar characteristics and challenges. First, attacks in both domains can be difficult to attribute. Cyber-intrusions and EM interference can be masked by the attacker or spoofed, that is, made to appear as though they are being carried out by a third-party. Another challenge shared with cyber is the dual-use nature of many space capabilities, which support both military and civilian customers simultaneously. Third, in both space and cyber, the destruction or disruption of capabilities usually does not lead to immediate and direct loss of human life; this may increase

[7] "Challenges to Security in Space"
[8] John Wolfsthal, "For Heaven's Sake: Why Would Russia Want To Nuke Space?" Federation of American Scientists, Feb 21 2024, https://fas.org/publication/russia-space-nuclear-weapons/

the risk tolerance of potential aggressors compared to attacks in the terrestrial domains with higher likelihood of human losses. Finally, both the space and cyber domains consist of steady-state competition below the level of armed conflict, such as constant probing by hostile actors of frequencies, networks, defenses, and responses. Adversaries also engage in regular low-level disruption of space and cyber networks, and employ directed energy "jamming" to blind sensors and disrupt communications to, from, and in space.[9]

Terminology

A brief review of important deterrence terminology is justified before proceeding to Part Two, beginning with the definition. The US Department of Defense (DOD) and NATO definitions share certain similarities but are not identical. The DOD Joint Definition for Deterrence is:

> *The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (JP 3-0)*[10]

NATO defines Deterrence as follows:

> *The convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act."*[11]

[9] Flanagan, Martin, Blanc, and Beauchamp-Mustafaga, 15-17.
[10] DOD Dictionary of Military and Associated Terms, United States Supreme Court, accessed 22 Mar 24, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.
[11] "NATOTerm," accessed November 21, 2023, https://nso.nato.int/natoterm/Web.mvc.

The two definitions share common features. "Action" in the DOD definition roughly equates to "coercion" in the NATO version.[12] Likewise, cost/benefit in DOD doctrine equates to consequences/potential gains for the NATO definition. The common themes relate to the deterrence concepts of *punishment* and *denial,* which will be explored shortly. The NATO definition includes an additional clause lacking in the DOD version; that is, "*a credible military capability and strategy with the clear political will to act*." This additional component relates to the concepts commonly referred to as the "Three Cs of Deterrence": Capability, Credibility, and Communication (the Three Cs will be further explored later in this section).

Punishment and Denial

The objective of deterrence is to convince an adversary to refrain from acting, which can be achieved either through punishment or denial. Deterrence by punishment is based on the threat of consequences for acts of aggression. Deterrence by denial seeks to convince the adversary that they cannot achieve their objectives through aggression. Denial strategies may include dissuading an aggressor with reassurances or "carrots". Dissuasion strategies seek to convince an aggressor that they can achieve more acceptable outcomes through inaction than through action. The critical factor in both punishment and denial/dissuasion strategies is the adversary's *perception of reality* and not any objective reality.[13]

The "Three Cs of Deterrence"

[12] In deterrence theory, "coercion" is the overarching concept under which deterrence and compellence reside. The difference between the two is subtle but important; whereas deterrence seeks to dissuade an adversary from acting, compellence aims to force an adversary to take a desired action. Thus, whereas deterrence generally applies in peacetime or pre-conflict, compellence generally applies during conflict. See Echevarria, A. Military Strategy: A Very Short Introduction, Oxford (New York) 2017, 47-50.

[13] Mazarr, Michael J., Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE295.html, 7.

Achieving effective deterrence requires Capability, Credibility, and Communication.[14] Influencing *perception* is critical; it is not enough simply to have the means to defend, retaliate, or threaten to do either. A defender must *convince* the adversary that they have the capability to inflict unacceptable pain (in the case of a punishment strategy), or to render any attack futile (in a denial strategy). This ability to influence the perception of the adversary is the basis for credibility. The aggressor must believe that the defender has both the capability to respond along with the *will* to do so. The final component necessary for deterrence is communication. The defender must communicate its deterrence objectives, that is, what it seeks to deter, and deterrence strategy, i.e. punishment, denial, or a combination of each.[15] Communication is not limited to proclamations but includes an array of activities to include military exercises, force posture, security cooperation with partners, and military operations throughout the continuum of conflict. Each of these activities can signal capability and credibility, but each activity can be made more effective when paired with a deliberate messaging strategy to highlight deterrence objectives whenever possible.

Integrated Deterrence (Narrow vs Broad)

Deterrence theory includes the concepts of narrow and broad deterrence. Narrow deterrence focuses on the threat of military force alone, whereas broad deterrence incorporates a "whole of government" approach. The concept of "integrated deterrence", the centerpiece of the 2022 US National Security Strategy, is an example of broad deterrence. Space deterrence is well

[14] In some publications, NATO substitutes *cohesion for "credibility"*; see Paulauskas, K, "On Deterrence" NATO Review, Aug 5, 2016, https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html.
[15] Mazarr, 9.

suited to a broad deterrence or integrated deterrence strategy for two reasons. First, assets in space are often exquisite and not generally attritable. Therefore, a defender would not seek to risk one's own assets by threatening to destroy an adversary's similar capabilities. Second, it is not in anyone's interest to take reciprocal actions in space, especially kinetic, as the effects of even successful counterattacks can have devastating second and third order effects to all space-faring nations.[16]

Alliance Deterrence

Deterrence theory addresses alliances primarily through the lens of "extended deterrence". A classical deterrence concept often referred to as the "nuclear umbrella", extended deterrence involves a "commitment to deter and, if necessary, to respond across the spectrum of potential nuclear and non-nuclear scenarios in defense of allies and partners."[17] NATO's Article 5 is an expression of extended deterrence in that an attack on one is to be construed as an attack on all. Extended deterrence applies to NATO space deterrence with an important caveat: Whereas with nuclear extended deterrence non-US NATO members are dependent on the US nuclear capability (France and the UK excepted), in space deterrence many allies bring unique national capabilities to the table. In other words, many countries are contributors to the extended deterrence regime as well as beneficiaries.

Alliances offer another type of deterrence advantage in that the multi-actor model complicates an aggressor's decision-making process; they must consider the potential response

[16] The incorporation of highly proliferated "mesh" satellite networks could soon mitigate this consideration, as on-orbit platforms become more "attritable" and less exquisite. However, even in the case of proliferated networks, countries may still wish to avoid being the first to launch a kinetic attack in space with potential harm to third countries and other non-beligerants.

[17] AFDP 3-72: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-72/3-72-D12-NUKE-OPS-Extended-Deterrence.pdf

of each member acting independently as well as the response of the alliance *as a whole*. Research shows that defensive alliances like NATO generally bolster overall deterrence effectiveness, making aggression against the alliance less likely.[18]

To conclude Part 1, the most important takeaway from deterrence theory can be succinctly summarized as follows:

> *Deterrence turns out to be about much more than merely threatening a potential adversary: It demands the nuanced shaping of perceptions so that an adversary sees the alternatives to aggression as more attractive than war.*
>
> - Michael Mazarr[19]

[18] Brett Ashley Leeds, "Do Alliances Deter Aggression? The Influence of Military Alliances on the Initiation of Militarized Interstate Disputes," *American Journal of Political Science* 47, no. 3 (July 1, 2003): 427–39.
[19] Mazarr, 2.

Part 2. Achieving Space Deterrence

Part 1 introduced deterrence theory in general and space deterrence specifically, Part 2 will explore what achieving space deterrence looks like in practice. It begins with a discussion of punishment and denial strategies for space deterrence, and then explore how the "Three Cs of Deterrence" – Capability, Credibility, and Communication – can be applied.

Punishment and Denial

Recall that when discussing "space deterrence", we mean deterrence in the narrow sense of dissuading a potential aggressor from taking hostile action against our space capabilities. Such a deterrence regime applies in both peacetime and in conflict. For example, deterring an adversary from anti-satellite (ASAT) attacks remains a viable goal even when engaged in large-scale conventional conflict. It is also a highly desirable goal given the widespread and long-term consequences of such an attack.

In the above scenario, achieving deterrence via punishment would require fostering a perception in the adversary that our response would be unacceptably painful, i.e. his situation would be worse than the *status quo ante*. With an "integrated deterrence" strategy, the punishment need not be conducted from space, nor on the aggressor's space capabilities. It could materialize from another military domain or a different instrument of power altogether. As an example, the punishment for an ASAT operation could be a cyber-attack against an adversary's coastal defense capabilities. A defender also does not need to specify the exact punishment ahead

of time for deterrence to be effective, only to convince the aggressor of the likelihood of unacceptable consequences.

A denial strategy for space deterrence is slightly more complicated, as there are at least three ways to achieve deterrence by denial:

1) Employing countermeasures at the point of attack. For example, shooting down a missile, or detecting and mitigating a cyber intrusion.
2) Building resilience into the capability, such as having a stand-by platform take over when a primary platform is destroyed, or switching between one network and another as necessary in a hostile EM environment (e.g. Galileo and GPS). Resilience measures may include disaggregation, distribution, diversification, proliferation, and deception.[20]
3) Rapidly reconstituting a space capability in the case of destruction.

Denial strategies achieve space deterrence by convincing the adversary that his contemplated attack will fail to achieve the objective due to defensive measures or resilience. Either would render an attack costly and ineffective and thus not worth pursuing.[21]

Denial and punishment strategies are complementary and mutually reinforcing. The aggressor must consider not only the punishment he will likely incur, but also that the attack may fail due to one of the denial factors above. In this case the cost-benefit calculus may shift decidedly in the defender's favor. For this reason, most countries adopt a mixed deterrence strategy for space.[22]

---

[20] Space Doctrine Note – Operations, Jan 2022, 14.
[21] Mazarr, 2.
[22] Flanagan, Martin, Blanc, and Beauchamp-Mustafaga, 22-36. "A Framework for Space Deterrence", 2023, 22-28. The study analyzed various countries' approaches to Space Deterrence and binned them into three categories, or "archetypes". Countries with a "Punishment Dominant" strategy included Russia and China, whose ASAT testing and on-orbit activities are likely intended to demonstrate their ability to inflict pain on an adversary. Those with a "Denial Dominant" strategy include France and Japan. Both countries seek to deter threats to their space capabilities primarily through norms-advocacy, and both limit their defensive space actions to targeting the terrestrial or link nodes of an adversary's capability, rather than on-orbit platforms. The authors place the US as well as India in the third category of "Mixed Deterrence", the countries rely about evenly on both punishment and denial strategies to achieve space deterrence.

Capability

For the purpose at hand, "capability" includes the functions and missions that enable a defender to achieve deterrence; in short, operational space capabilities. The subsequent section will focus on the concepts, policies, and other activities that support space operations. Commander of US Space Command identified the following capabilities as critical to space deterrence:[23]

- *Enhanced Battlespace Awareness for Space Warfare* – Deterrence starts with understanding the threat and what you are attempting to deter. Achieving a sufficient understanding of the threat requires a comprehensive awareness of the battlespace. This understanding must encompass not only the space domain but other domains where actions can achieve effects in the space domain, e.g. cyber threats to space enabled networks, and surface-to-space kinetic and non-kinetic capabilities. Countries should aspire to maximize their battlespace awareness however possible including through partnerships with civil government agencies, industry, academia, and allies and partners.

- *Resilient Space Command and Control* – All space capabilities should seek some level of resilience, but for Command and Control (particularly where C2 of nuclear forces is involved), resilience is a first-order necessity. Deterrence credibility could be questioned without reliable, assured, and resilient C2 of space assets or through space assets, e.g. SATCOM networks enabling C2 to distributed and dispersed ground, air, and naval forces.

- *Integrated Space Fires and Protection* – Space fires and protection capabilities enable deterrence by denial at the point of attack and contribute to denial by punishment where enemy space capabilities can be held at risk (e.g. on-orbit assets). Offensive-dominant deterrence strategies would incorporate greater terrestrial and/or on-orbit fires capabilities including lasers, missiles, and jamming. These capabilities can also be employed

[23] "Space Policy Review and Strategy on Protection of Satellites", Office of the Secretary of Defense, September 2023, 16-18, accessed online 10 Dec 2023, https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/COMPREHENSIVE-REPORT-FOR-RELEASE.PDF.

defensively to defeat an ongoing or pending attack. Electronic warfare (EW) and cyber are two subsets of Space Fires and Protection that deserve special attention.[24]

- *Modernized, Agile Electronic Warfare Architecture* – EW Architecture enables deterrence both though the identification of hostile EW activity as well as by providing a mechanism for protection and counterattack to bolster both denial and punishment strategies.

- *Space Systems Cyber Defense* – Space capabilities are highly dependent on cyber data networks and are thus vulnerable to cyber-attack. Cyber defenses provide operational *assurance* and complicate an aggressor's cost/benefit calculus, thus bolstering deterrence by denial. In the cyber domain, the best defense is often a superior offense along with the willingness to use it.

A final required capability is *rapid reconstitution of space capabilities*.[25] Rapid reconstitution is one of the three methods of achieving deterrence by denial. In the event of attack on a defender's military space assets, defenders must possess the ability to quickly replace the platform or capability/effect through dynamic space-lift or on-orbit spares, or by harnessing commercial or civil sector platforms to ensure continuity of operations in a conflict. Demonstration of such a capability complicates the risk calculus of a potential aggressor and thus enhance deterrence.

Credibility

While capabilities provide the mechanism for carrying out punishment threats or achieving denial at the point of attack, by themselves they do not provide the necessary

[24] *Space Doctrine Note – Operations,* Accessed Feb 20, 2024, https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/ SDN%20OPERATIONS%2025%20JANUARY%202022.PDF, 14. SDN-Operations identifies the four protection measures as Electromagnetic Spectrum Operations, Movement and Maneuver, Hardening, and Cybersecurity.
[25] Flanagan, Martin, Blanc, and Beauchamp-Mustafaga, 32-34.

credibility to achieve successful deterrence. Building space deterrence credibility starts with developing a coherent space policy, along with a reasonable and achievable strategy that ties one's capabilities to one's policy objectives. Credibility is further bolstered by crafting doctrine, "tactics, techniques and procedures" and other instructions, by educating and training the force, and by constantly improving concepts and capabilities through wargaming, exercises, and operations. These activities are not pursued with the objective of deterrence alone, but they bolster deterrence by developing and showcasing a capable space force. The space strategy should nest appropriately within higher level strategic guidance and providing a bridge to space doctrine. Robust, realistic, and up-to-date policy and strategy serve to bolster the Three Cs of deterrence. Policy, strategy, and all other guidance must be mutually reinforcing and unambiguous about the deterrence objectives sought.

Deterrence considerations for space policy:

- Recognizing the right to counter and disable hostile space activities and other threats
- Staking the right of mission assurance to/from/and in space
- Equating attacks on strategic space capabilities (MW, NC3) with strategic territorial attacks necessitating an equivalent response
- Stating that attacks on space assets will result in a response from/to any domain at a level commensurate or greater than the result of the attack (i.e. integrated deterrence)
- Acknowledging the norms and normative behavior to which space forces abide and operate
- Asserting counterspace "red lines" (ambiguous and/or unambiguous)[26]

Deterrence considerations for space strategy:

- Establishing the role of deterrence within the strategic objectives of Space Forces

[26] Ambiguous and unambiguous red lines each serve a purpose. The former eliminate any doubt in the mind of an aggressor that hostile action will incur a painful response e.g. "A *kinetic ASAT attack and will be met by a proportional or greater response in a domain and at a time of our choosing;*" the latter to foment doubt and complicate decision making, e.g. "*any attack on NATO space capabilities may be considered an attack necessitating an Article 5 response."*

- Specifying the deterrence paradigm sought – i.e. Offensive, Defensive, or Mixed
- Articulating objectives for space superiority/supremacy in conflict
- Asserting a theory of victory (or success)[27] for space forces
- Identifying escalation control considerations for counterspace operations
- Explaining how space forces are integrated with other domains in peace and conflict
    - Emphasize the essential role space forces and assets play in support of other military forces and government agencies and services
- Including deterrence as a Line of Effort tying capabilities to strategic objectives
    - Specify the capabilities that are integral to the deterrence Line of Effort
    - Tie space force operations, activities, and investments specifically to deterrence strategies, i.e. denial via platform redundancy, rapid relaunch, etc.

Space deterrence credibility also requires demonstrating that a country's space capability can be mustered, fielded, and operated to achieve its objectives. To demonstrate operational capability for deterrence purposes, space forces should:[28]

- Establish Doctrine - Establish doctrine for all space mission areas and functions, to support joint and combined space and multi-domain operations. Doctrine and TTPs should identify where and how space operations support space deterrence and wider deterrence strategies.

- Contribute to Planning – Participate in integrated planning at all levels to ensure space requirements, capabilities, and risks are captured.

- Organize for All-Domain/Multi-Domain Operations (MDO) – Structuring military organizations to effectively conduct multi-domain operations is key enabler for space deterrence. Specifically, integrating cyber and information warfare with space forces in a significant way would be highly effective in complicating an adversary's planning considerations that the joint/combined force is adequately protecting its organizational flanks, and eliminating any seams between the terrestrial and non-terrestrial domains. Organizing for MDO is particularly important in deterring "grey zone" and hybrid threats to friendly forces and societies.

---

[27] Billy Blankenship, "Space Force Leaders Take On Air University", Air University Press, Published Jan 24, 2024, https://www.spaceforce.mil/News/Article-Display/Article/3656855/space-force-leaders-take-on-air-university/ , USSF Chief of Space Operations Gen Chance Saltzman introduced the US Space Force Theory of Success - Competitive Endurance, in 2023. He further explained in Jan 2024 at Air War College that he does not see a clear end-point in the competition in space, and that competition is preferable to conflict in space; hence "theory of success" rather than "theory of victory".

[28] Flanagan, Martin, Blanc, and Beauchamp-Mustafaga, 30-36. The ideas from the subparagraphs below come principally from the "Framework for Deterrence in Space" report.

- Participate in Exercises - Conduct regular exercises at Service, Joint and Combined levels to demonstrate and operationalize emerging space and MDO concepts. Exercise planning must involve appropriate space experts to ensure realistic warfighting scenarios that include environments with degraded, disrupted, and or destroyed space capabilities.

- Conduct Operations – The most effective communication of *potential* capability is the demonstration of *existing* capability through the execution of space operations. While policymakers and governments may wish to conceal certain capabilities to prevent an adversary from developing countermeasures and preserve the element of surprise, deterrence requires the demonstration of military space and counterspace capabilities to potential adversaries.

Communication

Communication includes policymakers' public statements, communiques, and verbal and written issuances of all types. Signaling capability and credibility through force posture and military activities comprise an equally important mechanism for deterrence communication. Many of the activities addressed in the "Credibility" section are effective means of signaling, and thus communicating. The important thing is to ensure that all communication messaging and signaling is coherent and consistent. In other words, government statements echo published strategy and policy, which in turn supports doctrine and tactics, and that exercises and operations are conducted in a manner consistent with all of the above.

Examples of how military exercises can be used for deterrence messaging include:

- Including non-traditional allies and partners such as out-of-area countries and Intergovernmental Organizations (IGO) – Increases resilience of defender's space capability through access to unexpected military partners. (*Denial)*

- Integrating commercial and civil/IGO platforms into exercise scenarios – Increases resilience of defender's space capability through access to unexpected non-military partners. *(Denial)*

- Demonstrating "integrated deterrence" by simulating effects using non-military instruments of power – Increases scope of retaliatory possibilities that an aggressor must plan for. *(Punishment)*

- Incorporating senior civilian decisionmakers in tabletop exercises – When properly captured and communicated, such integration signals to the adversary that the *political will* exists. *(Punishment)*

Space forces should also incorporate information operations specialists to ensure the intended messaging is being communicated through all strategic communications and operational activities. Finally, space forces public affairs teams must complete the communication circle through press releases and other outreach, by showcasing the linkages between space policy and operations, activities, and investments, in support of deterrence objectives.

The measures above provide an extensive menu of deterrence options that should be considered by any space-faring nation or alliance interested in space deterrence. In Part Three, we will adapt the proposed measures specifically to the NATO space enterprise.

Part 3. NATO Space Deterrence

The NATO Space enterprise takes its strategic direction from two sources, the NATO Overarching Space Policy (published January 2022) and the NATO Strategic Concept (published June 2022). These documents consolidate a decade of NATO thinking and public statements on space and provide a foundation for the recommendations that follow.

Overarching Space Policy

NATO's Overarching Space Policy establishes the alliance's specific space equities and approach to space operations. It establishes space as an operational domain and emphasizes the essentiality of space to NATO deterrence and defense, and to terrestrial military operations.[29] The Policy explicitly identifies the counterspace threat as follows:

> *The capabilities being developed by potential adversaries could be used against the Alliance [to] hold space assets at risk, thereby complicating NATO's ability to take decisive action in a crisis or conflict; deny or degrade Allies' and NATO space-based capabilities critical to battlespace management and situational awareness and the ability to operate effectively in a crisis or conflict; create impacts on Allies' space systems that are damaging or disruptive to economic or public life and violate the principle of free use of space, yet fall below the thresholds of threat of force, use of force, armed attack or aggression.*[30]

The Policy identifies NATO Space equities comprising four key roles:[31]

1. Integrating space into the delivery of NATO's core tasks
2. Serving as a forum for political-military consultations on deterrence and defense-related space developments

[29] *NATO Overarching Space Policy,* North Atlantic Treaty Organization, Last updated 17 Jan 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.
[30] *NATO Overarching Space Policy,* paragraph 2.
[31] *NATO Overarching Space Policy,* Paragraph 6.

3. Ensuring effective provision of space support and effects to the Alliance's operations, missions, and other activities
4. Facilitating compatibility and interoperability between Allies' space services, products, and capabilities

In support of its approach, the Policy specifies six functional areas that requiring NATO space systems: Space Situational Awareness, Space-enabled Intelligence Surveillance and Reconnaissance, Space-based Environmental Monitoring, Satellite Communications, Position Navigation and Timing, and Shared Early Warning. These functional areas constitute what are often referred to a "space services" and notably exclude warfighting capabilities otherwise known as "space control" or "counterspace operations."

Paragraph 5 of the Policy specifies that NATO is not "aiming to be an autonomous space actor" nor "to develop space capabilities of its own". To be sure, the policy does not *proscribe* NATO commanders' operation or control of space-based assets. The Policy also addresses commercial augmentation in the space domain: "Allies' capabilities, and, if necessary, trusted commercial service providers should be leveraged to meet these requirements in the most secure, efficient, effective and transparent manner."[32]

The Policy was drafted and published prior to Russia's February 2022 invasion of Ukraine. While useful and comprehensive, it unfortunately reflects an approach to space that does not do justice to the counterspace threat that NATO currently faces. It also discounts the offensive and defensive space capabilities available to NATO to respond to the counterspace threat. In short, the Policy continues to view space through a functional lens of "support to military operations" rather than a true warfighting domain. The phrasing in much of the Policy

[32] *NATO Overarching Space Policy,* Paragraph 8.

appears designed to accommodate differences among alliance members over the extent of NATO's role in space operations.

Strategic Concept

The NATO Strategic Concept – published in the wake of Russia's invasion of Ukraine – bolsters the Overarching Space Policy in at least four ways. 1) It reaffirms the alliance's three core tasks: deterrence and defense, crisis prevention, and cooperative security. 2) It pledges NATO to "significantly strengthen our deterrence and defense posture to deny any potential adversary any possible opportunities for aggression."[33] 3) It identifies Russia and China specifically, and authoritarian actors more generally, as the primary threats to Euro-Atlantic and global security, citing these "malign actors" as engaging in a constant effort to degrade, disrupt and target NATO capabilities in cyber and space.[34] And 4) it embraces a mixed deterrence strategy, utilizing both *punishment* and *denial* elements:

> *A single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty* [punishment]…*We will also boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security* [denial].[35]

The Concept also embraces the paradigm of broad or "integrated" deterrence, both for space as well as for nuclear deterrence:

[33] *NATO 2022 Strategic Concept,* North Atlantic Treaty Organization, accessed 10 Dec 2023; https://www.nato.int/strategic-concept/, 6.
[34] *NATO 2022 Strategic Concept,* 2-5
[35] *NATO 2022 Strategic Concept,* 7.

> *The Alliance is committed to ensuring greater integration and coherence of capabilities and activities across all domains and the spectrum of conflict, while reaffirming the unique and distinct role of nuclear deterrence. NATO will continue to maintain credible deterrence, strengthen its strategic communications, enhance the effectiveness of its exercises and reduce strategic risks.*[36]

Together, the Policy and Concept, coupled with regular strategic messaging such as Communiques,[37] provide a useful foundation for NATO space deterrence. In the next and final section, we will identify potential capabilities and measures to enhance NATO space deterrence. While most of the options offered are compatible with the existing guidance, any tensions will be identified and addressed.

Recommendations for NATO Space Deterrence

Capability

It is important to reiterate up front that when speaking of "NATO capabilities", with few exceptions these are not owned and operated by the Alliance itself, but rather are *presented to* NATO as part of the multinational force generation process.[38] As an alliance, NATO draws on the capabilities of its 32 member nations as well as a small cadre of NATO forces assigned to the NATO Space Center at Ramstein. The Center "delivers regular analysis to support NATO's

[36] *NATO 2022 Strategic Concept,* 8.

[37] The alliance releases communiques after high-level meetings and summits. These communiques sometimes advance space deterrence objectives. For example, the 2021 Brussels Communique recognized that attacks to, from, or within space could present a clear challenge to the security of the Alliance and could lead to the invocation of Article 5 of the North Atlantic Treaty. This tenet was later adopted in the 2022 Strategic Concept.

[38] While network architectures are either presented to NATO through the force generation process or jointly developed through common funding, space products, data and other services are generally provided through bilateral agreements between NATO and individual alliance members, as well as between NATO and non-member states, government-civilian agencies, and non-government commercial, scientific, and academic organizations.

situational awareness and decision-making," ingesting data and information from contributing members and a limited number of commercial providers.[39] Going forward, NATO must expand these efforts and grow its operational capacity to meet the deterrence and defense requirements of the recently approved regional defense plans.[40] All opportunities for formal and informal partnerships involving member and non-member military, civilian, intergovernmental (e.g. EU) and commercial institutions should be explored, as potential contributors to NATO resilience. The paragraphs below adapt the specific capability recommendations from Part 2 to the NATO context.

- *Enhanced Battlespace Awareness* – NATO should leverage all member states military and non-military space domain awareness (SDA) data to maximize battlespace awareness. Emphasize the mutual interest in responsible use of space and safety of space operations to encourage maximum participation by NATO partners, civilian, commercial, scientific, and academic entities to exchange potentially sensitive and proprietary information. NATO must integrate ground and space-based SDA capabilities, encompassing all orbital regimes and key terrain in space. NATO's Allied Persistent Surveillance from Space (APSS) - "a virtual constellation…of both national and commercial space assets"[41]- is one promising avenue of Enhanced Battlespace Awareness for the alliance. NATO participation in USSPACECOM's Joint Commercial Office (JCO) is another potential avenue for enhanced battlespace awareness. NATO as an alliance is also ideally suited to enhance battlespace awareness through space forensics, developing a cadre of experts to analyze, identify, and expose nefarious activities in space that violate international norms and agreements.

- *Resilient Space Command and Control* – To bolster legacy space command and control (and communication) networks, NATO could contract with commercial providers offering mesh networks utilizing LEO constellations to provide secure and survivable data-transport layers. NATO could also consider bolstering and improving terrestrial linkages between uplink/downlink nodes (civilian and military) to ensure resilience in the event of successful adversary counterspace targeting through EW, cyber or conventional attacks.

- *Integrated Space Fires and Protection* – NATO forces must be able to defend against adversary attempts to deny/degrade/disrupt and or destroy space-enabled operational capabilities including SATCOM, P&T, C4ISR, etc. Therefore, counterspace or "space

[39] Jens Stoltenberg, Secretary General's 2023 Annual Report, NATO, 2024, accessed Mar 20, 2024, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/sgar23-en.pdf, 31
[40] Stoltenberg, 23-39.
[41] Stoltenberg, 78.

defense" capabilities must be adequately incorporated into all NATO planning, wargames and exercises at all military echelons to include the strategic decision-maker level (i.e. NATO Ambassadors). As space operations are cyber intensive, consider establishing space/cyber/IO cells within tactical units and multinational brigade headquarters to coordinate counterspace effects in support of deterrence and defense objectives.

- *Rapid Reconstitution* – While NATO will not "own" on-orbit assets for the foreseeable future, it can bolster rapid reconstitution by coordinating the development of space-lift capacity and resilient terrestrial capability (including rockets, fuel, storage/maintenance facilities, etc.) throughout alliance territory. NATO can also bolster rapid reconstitution capacity through improved movement via air/land/sea of space assets prior to launch. These capabilities should be considered as part of regional defense and crisis planning. Finally, NATO should conclude agreements with commercial and civilian partners to enable reconstitution of space-based services when the alliance's military capabilities are denied, degraded, disrupted, or destroyed.

Credibility

Space deterrence credibility can be enhanced in the areas of Guidance (Policy, Strategy and Doctrine), Space Forces Integration, and Exercises and training.

Update Policy

NATO must increase its ambition for space in light of the new Strategic Concept and Deterrence and Defense of the Alliance (DDA) construct.[42] With ever-increasing threats in, from, and to space, it is high time for NATO to declare a policy of active defense of its members' space assets and alliance space equities, utilizing all capabilities available. It should expand its "key roles" and functional areas to include space warfighting roles. To build alliance consensus, NATO might consider adopting the term "space defense" rather than "space control" or "counterspace." This would keep the terminology in line with NATO's first core task of

[42] "Deterrence and Defense", NATO, last updated Oct 10, 2023, https://www.nato.int/cps/en/natohq/topics_133127.htm.

"Deterrence and Defense" and would align with existing NATO missions such as Integrated Air and Missile Defense (IAMD).[43]

Integrate Space Warfighters

The best way for NATO to transition to credible space deterrence is through employing space warfighters throughout its force structure. While the NATO Space Center serves as a useful tool to integrate and direct space contributions such as SDA and SATCOM from allied members and partners, the alliance must integrate space defense operators into its Multinational Battlegroups and Allied Response Force structures to provide steady state space defense capabilities and to be ready at the outset for any expanded conflict in Europe. NATO should capitalize on the Allied Command Transformation's Multi-Domain Operations Concept[44] to ensure the future force structure integrates space warfighters at every echelon and throughout extent of alliance missions.

Create Strategy, Doctrine, and Standards

NATO must develop a space strategy on par with those of the terrestrial domains. Such a strategy would acknowledge the requirement for NATO space forces to conduct all-domain operations and "space defense" operations in support of NATOs regional defense plans. A NATO space strategy would demonstrate alliance *credibility* by articulating the ways and means for achieving its space policy ambitions, clarifying the role of the NATO space enterprise in crisis and conflict, and providing direction to member states for prioritization of space capability

[43] "NATO Integrated Air and Missile Defense", NATO, Last Updated 13 June 2023, https://www.nato.int/cps/en/natohq/topics_8206.htm.
[44] "Multidomain Operations in NATO – Explained", NATO ACT, Oct 5, 2023, https://www.act.nato.int/article/mdo-in-nato-explained/.

investments and contributions to the alliance. By articulating the "ways and means" for utilization of space forces and prioritizing space missions and investments, a strategy would also serve as a roadmap for planning and doctrine development. NATO doctrine should be developed to address the roles and responsibilities for the NATO Space Center and all space-integrated units, as well as ADCON/TACON relationships both internal and external to the NATO force structure. NATO must also establish common standards for space data and C4 architectures to maximize interoperability of alliance member and partner space data, products, networks, and services. These efforts would further enhance space resilience and reconstitution capability, thus bolstering deterrence by denial.

Conduct Space Exercises

NATO should demonstrate credible capability and political will through regular exercises at all echelons incorporating the entire range of adversary counterspace operations from localized degradation to nuclear detonation in space. Exercises should include integration of non-alliance civilian and commercial capabilities along with measures to protect and defend such capabilities in the event of crisis or conflict. In planning future exercises, consider incorporating:

- Degraded, disrupted, and denied military space-services in tactical/operational field exercises and strategic table-top exercises; e.g. NUDET scenario for Ambassador-level wargame
- Civilian space resilience measures to include European Union/European Space Agency capabilities
- Commercial space resilience measures
- "Integrated deterrence" response options, including multi-domain and non-military instruments of power

Communication

NATO maintains robust and highly effective overt messaging capabilities. To enhance space deterrence, however, NATO must utilize these mechanisms to clearly express its deterrence objectives. Messaging should articulate both what NATO seeks to deter – aggression against space assets and capabilities – along with a commitment to meet any transgression with a painful response. Messaging considerations may include:

- Clearly declare NATOs intent to deter counterspace threats using both punishment and denial mechanisms
- Identify space-deterrence and defense capabilities through both messaging and signaling, i.e. *punishment* through space defense (or counterspace operations) and *denial* through resilience and reconstitution
- Clearly establish ambiguous and/or unambiguous red-lines within the counterspace threat continuum.[45]
- Consider "integrated deterrence" messaging options
- Signal space-deterrence intent by integrating space forces into the multinational brigades and showcasing space-integrated multi-domain operations in exercises and operations.

Norms

As a multilateral alliance of democratic states, NATO's voice carries significant weight, and the alliance should continue to advocate regularly for the peaceful and responsible use of space through its own messaging. Efforts to normalize responsible behavior in space indirectly support deterrence by delegitimizing threatening activity prior to a period of crisis. Establishing norms also enhances deterrence by increasing the likelihood that aggression against one country's space assets would rally a multinational response from sympathetic like-minded countries. Actions NATO could consider in this area include becoming an observing member of the Combined Space Operations (CsPO) forum and a signatory to the Artemis Accords. NATO can further contribute to enhancing norms by ensuring that all operations, activities, and

[45] See earlier note that discusses the justification for ambiguous vs unambiguous red lines.

investments NATO takes with other countries and institutions include a stated commitment to responsible behaviors in space.[46]

Conclusion

Reflecting the current environment of rapidly advancing counterspace threats, this paper intended to offer useful recommendations that NATO could adopt to strengthen its space deterrence posture. It provided an overview of deterrence theory, emphasizing how space deterrence compares with cyber and nuclear deterrence. It then discussed what space deterrence looks like in practice for an individual spacefaring nation. The final section provided an overview on NATO's space enterprise and then adapted space deterrence concepts and critical requirements to the alliance. Key takeaways in the form of recommendations for improving NATO space deterrence include: 1) NATO should embrace "space defense" as a key role of the alliance; 2) NATO should develop strategy and doctrine to implement a mixed space deterrence strategy including space defense and resilience measures; 3) NATO should integrate space forces into its standing force structures (Multinational Battlegroups and the Alliance Response Force); and 4) NATO should integrate the full spectrum of counterspace threats into exercises at all echelons. Future researchers or practitioners may find this paper useful as a baseline for the development of a "NATO Space Strategy" that fully integrates NATO space into the alliance's regional planning and "Deterrence and Defense" mission areas.

[46] Flanagan, Martin, Blanc, and Beauchamp-Mustafaga, 36.

BIBLIOGRAPHY

Blankenship, Billy "Space Force Leaders Take On Air University", Air University Press, Published Jan 24, 2024, https://www.spaceforce.mil/News/Article-Display/Article/3656855/space-force-leaders-take-on-air-university/.

"Case Study: Viasat" Cyber Peace Institute, accessed Dec 10, 2023, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

"Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion" Defense Intelligence Agency, 2022, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/ Challenges_Security_Space_2022.pdf.

"Competing in Space", NSIC, Air Force Public Affairs, 2023

"Deterrence and Defense", NATO, last updated Oct 10, 2023, https://www.nato.int/cps/en/natohq/topics_133127.htm.

"DOD Dictionary of Military and Associated Terms," United States Supreme Court, accessed 22 Mar 24, https:// www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.

Echevarria, Antulio. "Military Strategy: A Very Short Introduction," Oxford (New York) 2017, 47-50.

"Extended Deterrence," AFDP 3-72, Curtis E. Lemay Center, Last Updated Dec 18, 2020, https:// www.doctrine.af.mil/Portals/61/documents/AFDP_3-72/3-72-D12-NUKE-OPS-Extended-Deterrence.pdf

Flanagan, Stephen J., Nicholas Martin, Alexis A. Blanc, and Nathan Beauchamp-Mustafaga, "A Framework of Deterrence in Space Operations," Santa Monica, CA: RAND Corporation, 2023. https:// www.rand.org/pubs/research_reports/RRA820-1.html.

Leeds, Brett Ashley, "Do Alliances Deter Aggression? The Influence of Military Alliances on the Initiation of Militarized Interstate Disputes," *American Journal of Political Science* 47, no. 3 (July 1, 2003): 427–39.

"Lift Off: NATO Launches New Space Center of Excellence," NATO ACT, accessed March 24, 2022, 2024, https:// www.act.nato.int/article/space-newest-coe/

Mazarr, Michael J., Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018. https:// www.rand.org/pubs/perspectives/PE295.html.

"NATO 2022 Strategic Concept," North Atlantic Treaty Organization, accessed 10 Dec 2023, https:// www.nato.int/strategic-concept/.

"NATO Integrated Air and Missile Defense", NATO, Last Updated 13 June 2023, https://www.nato.int/cps/en/natohq/topics_8206.htm.

"NATO Overarching Space Policy," North Atlantic Treaty Organization, Last updated 17 Jan 2022, https:// www.nato.int/cps/en/natohq/official_texts_190862.htm.

"NATOTerm," accessed November 21, 2023, https://nso.nato.int/natoterm/Web.mvc.

Paulauskas, Kestulis, "On Deterrence," NATO Review, Aug 5, 2016, https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html.

Space Doctrine Note – Operations, Accessed Feb 20, 2024, https://media.defense.gov/2022/Feb/02/ 2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF.

"Space Policy Review and Strategy on Protection of Satellites", Office of the Secretary of Defense, September 2023, 16-18, accessed online 10 Dec 2023, https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/COMPREHENSIVE-REPORT-FOR-RELEASE.PDF.

Stoltenberg, Jens, Secretary General's 2023 Annual Report, NATO, 2024, accessed Mar 20, 2024, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/sgar23-en.pdf.

Wolfsthal, John, "For Heaven's Sake: Why Would Russia Want To Nuke Space?" Federation of American Scientists, Feb 21 2024, https://fas.org/publication/russia-space-nuclear-weapons/.