NATO's Space Deterrence Dilemma

Lilla DOUCHA
Junior Researcher
Institute for American Studies at Ludovika
Budapest, Ludovika tér 2, 1083 HUNGARY

Doucha.Lilla@uni-nke.hu

ABSTRACT

Can improved Space Situational Awareness (SSA) broaden the scope of space deterrence's credible applicability? To establish the opportunities granted by the development of SSA, first the implementability of NATO's space deterrence will come under scrutiny. Thus, the first section of the paper will be dedicated to the importance of space deterrence in light of the recurring arms race, the potential alternative strategies, and the requirements of credible deterrence in the fifth domain. Followingly, the an escalation ladder of intentional space threats and a case selecting analysis will be carried out. Two hypotheses will be tested; (1) deterrence by punishment can be credibly applied in the outer space under certain conditions; and that (2) deterrence by denial can be credibly applied in the outer space under certain conditions. Finally, the analysis of variables and particular conditions sufficient for credible space deterrence will be undertaken. The second part of the paper will address the gaps identified during the first round of analysis by exploring the opportunities SSA development can present. A summary of findings will reflect on whether improved SSA can contribute to the extension of space deterrence's scope.

1. INTRODUCTION - THE IMPORTANCE OF SPACE DETERRENCE

1.1. Growing reliance on space

"Space is a dynamic and rapidly evolving area, which is essential to the Alliance's deterrence and defence".[1] The importance of the security of NATO space capabilities and services[2] has grown with the increasing reliance on space as an operational enabler and enhancer. Satellites of communication, navigation and intelligence became embedded into the critical infrastructure of Allied nations. But despite the vital role space plays in civilian and military activities, space systems tend to be highly vulnerable and exposed to degradation. The physical constraints of the domain and the dependence on sophisticated, hardly reparable or replaceable technology forces NATO to face a number of manmade security and natural safety hazards. Electrostatic discharge, loss of fuel, solar storms, and meteor showers account for some of the naturally occurring[3] menaces leading to satellite failure.[4] On top of these accidents, electromagnetic interference from other adjacent satellites, and collision with space debris pose human activity-derived risks to space objects.[5] This exposure of orbiting assets is furthered by the threat of intentional degradation or destruction from adversarial attacks.

While NATO was no stranger to space operations since the launch of the NATO1 communications satellite in 1970,[6] the official recognition of the importance of outer space for the Alliance was delayed until the

[1] NATO, "NATO's approach to space," para 1.
[2] All references to NATO's space assets and capabilities are purposeful simplifications as NATO itself does not possess space technologies. All space systems except for a few ground stations are in the ownership of Allied nations or procured from commercial services. ACT, "NATO's New Space Policy."
[3] In terms of without intentional interference.
[4] Gould and Orin, *Estimating Satellite Insurance Liabilities*, 54-56.
[5] European Space Agency, "Detecting Space Hazards," 11.
[6] Tombarge, "NATO Space Operations."

Brussels Summit in 2018.[7] The continuation of the Summit's commitment to space was materialized a year later through the adoption of a classified internal strategy. NATO's Space Policy was then followed by the London Summit's declaration on space as the fifth operational domain along land, sea, air, and cyber.[8] Followingly, Defence Ministers agreed on the establishment of a Space Centre as part of the Allied Air Command in Ramstein.[9]

Then in 2021 the Brussels Summit declaration extended the scope of Article 5 – also referred to as the common defence clause – to the space domain.[10] The decision to trespass the geographic demarcations of Article 6[11] demonstrated that the Alliance is ready to undertake the maintenance of collective security in the fifth domain. Since then "an attack on the space assets of any one Ally impacts the security of all Allies,"[12] creating effective means to protect Allied activities in space is in the interest of all 30 member states.

1.2. Militarization of space

The threats posed to the Alliance's security are significantly different today than during the first era of space race. Unlike in the days of the Cold War, today the technology capable of interfering with satellites is not limited to the two superpowers.[13] Moreover, with the first Gulf War in 1991 space emerged as a significant enhancer of military operations, which showed a clear divergence from the former symbolic role of operations in space.[14] This growth in strategic value of space assets placed an increased emphasis on preventing unfriendly nations from resorting to the use of force against orbiting capabilities. As the categorization of assets will demonstrate, diminishing the Alliance's space support can lead to severe deterioration of Allied nations' defence and warfighting capabilities across every domain. Thus, transatlantic Allies need to seek effective ways to guarantee the security of their assets in the space domain. Although to date space historic records do not note violent interstate encounters resulting in the destruction of a satellite,[15] power demonstrations have already taken place.[16] With the intensifying great power competition on Earth[17] and the proliferation of offensive space capabilities, the door to the first attack on an adversary's satellite remains widely open. Thus, capabilities providing security for allied space support are essential in the offense dominant domain of the outer space where defending an asset is considered harder than attacking one.[18]

[7] NATO, "Brussels Summit Communiqué," para 33.
[8] NATO, "London Declaration," para 6.
[9] NATO, "NATO Defence Ministers," para 3.
[10] NATO, "NATO's Overarching Space Policy," para 12.
[11] "For the purpose of Article 5, an armed attack on one or more of the Parties is deemed to include an armed attack:on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France 2, on the territory of Turkey or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer; on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer." NATO, *The North Atlantic Treaty*, para 6.
[12] Schulte, "Protecting NATO's advantage in space," 4.
[13] Non-state actors also have a seat at the table, however, "deterring non-state actors are virtually impossible," therefore present paper does not include they. Kopeć, "Space Deterrence: In Search," 124
[14] The Gulf War is often referred as the first space war due to the tremendous role of space services in support of the coalition operations. Greenemeier, "GPS and the World's First "Space War".
[15] Information on reversible interferences could not be accessed by the author due to classification.
[16] Since 1968 15 anti-satellite tests have been convened successfully by four states. Bhutada, "Anti-Satellite Weapons."
[17] Allison, "Destined for War?," 9-21.
[18] Gleason, "Getting the most deterrent value," 2.

1.3. How can NATO avoid conflict in space?

The unsuccessful attempts of the last decades to adopt legally binding treaties on space activities drove spacefaring nations towards establishing "norms of responsible behavior" to limit the chances of a space conflict.[19] However, "it's widely accepted that the current state of norms of behavior governing space activities is struggling to keep pace with the increasingly rapid innovation and diversification of space activities."[20] As such, the normative framework at this stage represents the wishful thinking of spacefaring nations without a potential unable to limit the aggressive behavior of spacefaring nations.

The most important of the five United Nations treaties,[21] Outer Space Treaty (OST) provides a more substantial contribution to upholding international peace and security. Its Article IV prohibition on deploying nuclear weapons and weapons of mass destruction intends to limit the chances of a destructive spacewar.[22] "A major problem of the treaty, however, is its lack of enforcement mechanism and no defined threshold for what constitutes a violation that sometimes give way to infringements."[23] Thus, the legal constraints of the international treaties fail to limit reckless state behavior. Moreover, the weakening cooperation among nations suggests that space is moving away from a system of space governance towards a state resembling anarchy.[24]

The relative underregulation and the discontinuation of projects between major space powers reinvigorates rivalry and insecurity in the high frontier.[25] In light of these dynamics, the strategy of "discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing his prospective gains" is increasingly gaining traction.[26] Albeit deterrence presupposes the presence of both offensive and defensive military capabilities in space, and thereby partially contradicts to the declaration that "NATO has no intention to put weapons in space,"[27] currently no alternatives outperform deterrence in its ability to prevent conflict in space.

1.4. Are there really no alternatives to deterrence?

Two alternative strategies set their foot in the literature; space control and space avoidance.[28] Nevertheless, none of them can offer more feasible solution to the security of space assets than deterrence. The idea of space control – building on the ability to secure access to space for friendly nations while denying it from adversaries – fails for legal and practical purposes. Monopolizing access to extraterrestrial spaces would violate Article I of the OST on the freedom of exploration and use of space by all states, and therefore deviate from NATO's traditionally emphasized adherence to International Law.[29] On a more practical note, denying access would require the development of robust capabilities to counter and rebut adversaries' attempts to launch their assets into orbit – including protagonist spacefaring nations like Russia and China. These actions would be at odds with NATO's intention of "maintaining secure use of and unfettered access

[19] Rose, "Safeguarding the heavens," 2.
[20] Johnson, "Insight – Developing Norms." Moreover, H.E. Armel Kerrest responded me on the question of "What legal enforcement mechanisms are in force for space law?" with a sour "None." Kerrest, *Outer Space Treaty."*
[21] The other four are the Rescue Agreement, the Liability Convention, the Registration Convention, and the Moon Agreement. Bartóki-Gönczy, "Az Űrtevékenységek," 94-95.
[22] United Nations General Assembly, *Outer Space Treaty*, Article IV.
[23] Ishola et al, "Legal Enforceability," 34.
[24] This process is echoed by Harrison et al, *Space Threat Assessment*, IV.
[25] Like the end of the international cooperation on the International Space Station between the United States and Russia. Chang, "Russia Says It Will Quit".
[26] Snyder, *Deterrence and Defense*, 3.
[27] NATO, "NATO's Approach to Space," para 5.
[28] Coletta, "Space and Deterrence," 171.
[29] NATO, "Madrid Summit Declaration," para 2.

to space"[30] and place an enormous burden on the Allied defence expenditure, which already struggled to reach the targeted 2% even without such expenses.[31]

The other alternative, space avoidance presents an even less viable option for Allied space strategy as it promotes the avoidance of heavily relying on space support. Turning away from space support is not only unlikely but also implausible as "space systems enable our modern way of war… without them, many of our most important military advantages evaporate. Today we rely on space for almost everything we do."[32] Currently NATO nations possess over 60% of orbiting satellites,[33] which does not only indicate that the organization uses an immense space infrastructure for its operational enablement and enhancement, but that Allies rely on space support disproportionately more than their adversaries. As a result, space proves to be a double-edged sword: while the benefits of orbiting assets is unmatched, the heavy reliance on them brings this operational domain to the center of adversaries 'attention. The asymmetry between any aggressor and NATO countries sets the Alliance into a position where it has more to lose than any challenger. Thus, a capable enemy can obtain significant benefits by making one or more Allied space assets non-functioning. Preventing such a detrimental outcome seems to be by no means possible via abandoning space support and the benefits provided by Allied assets.

In the absence of any strategies for coping with threats in the space domain, deterring an adversary from committing to an attack against space or ground-based space systems tends to be the only viable option.

1.5. Requirements of credible space deterrence

Deterrence becomes credible if the threat or denial is believed by the challenger who therefore refrains from carrying out an attack.[34] To achieve this credibly, deterrence must be able to successfully alter the enemy's anticipated cost-benefit analysis, and thereby prevent undesired actions. An attack on Allied space assets would indicate the failure of proving that NATO has the technological superiority or resilient capability to deny the gains from a violent encounter or to respond in a way that costs more to the attacker than the benefits attained.[35] Promoting this calculation requires a fine balancing from the Alliance's official communication between presenting the defensive and offensive capabilities of space assets and classifying sensitive details to retain the technological and strategic advantage.[36] Moreover, credible deterrence requires reliable attribution.[37] Without the ability to transparently[38] and timely determine the agent responsible for the attack, the aggressor can easily shirk the responsibility for the caused damage.[39] Thus, attribution is crucial for signaling a resolve to carry out deterrence in a rational and timely manner and thereby modify the adversary's anticipated payoff.[40]

However, the lack of violence does not automatically indicate that deterrence can be successfully implemented as other factors, such as the low strategic value of an asset, the absence of offensive

[30] NATO, "Strategic Concept," para 25.
[31] NATO Secretary General, "Annual Report," 141.
[32] Lynn III, *A Military Strategy*, 7-10.
[33] As of 1 January, 2022. The vast majority of those assets belonged to the United States. Statista, "Number of satellites."
[34] Zagare, "Classical deterrence theory," 375.
[35] Throughout the paper deterrence is interpreted on a binary scale; it either succeeds to deter aggression of any level with any type of attack, or short of that fails. Kaufmann, "The Requirements of Deterrence."
[36] As Silverstein noted, "Even if NATO issued unambiguous classified guidance or Allies privately share an understanding of how to apply collective defense in space, a classified internal policy cannot communicate credible resolve to an adversary." Silverstein, "NATO's Return to Space."
[37] Raymond, "International Cooperation," 221.
[38] Attribution information needs to be ready to disclosed to Allied partners, national decision-makers, and involved stakeholders to embrace credibility. Johnson-Freese, *Space Warfare*, 85.
[39] von der Dunk, "Liability versus Responsibility," 363.
[40] Gleason, "Getting the most deterrent value," 3-5.

capabilities, or other external circumstances restricting the operation can equally prevent antagonists from resorting to the use of force in space. Therefore, the following section will focus on whether deterrence can alter the cost-benefit calculations of adversaries in case of particular assets and thereby protect these capabilities. But first, the threats to NATO's assets will be presented for a better understanding of what the Alliance is facing with.

2. EXPLORING THE LIMITS OF SPACE DETERRENCE

2.1. Threats to be deterred

Counterspace measures can be categorized into reversible and non-reversible attacks.[41] While the goal of the former actions is to disable, deceive, disrupt, deny information and services, the latter focuses on physically degrading or destroying the target.[42] Electronic and cyber interferences such as harassing, blurring, temporarily blinding optics (dazzling), jamming (noising the signal), spoofing (sending false signals), meaconing (retransmission of signals)[43] and cyber attacks manipulating the information exchange between operation units and orbiting spacecrafts compose non-kinetic, reversible attacks.[44] These simple, cost-effective and easily attainable technologies do not even need to complete their mission 100% to cause disruption to the service of NATO's capabilities. As they operate without leaving traces, attributing aggressors is serious challenge.

Non-reversible attacks, like direct-ascent weapons launched to crash into the targeted satellite, rendezvous and proximity operations diverting satellites to abandoned orbits ("graveyards"),[45] interceptors and pre-positioned space mines cause physical degradation or destruction and generate hazardous space debris.[46]

Moreover, the distinction between the two categories is shadowed by dual-use technologies capable of both reversible and kinetic attacks. Directed energy weapons, located mainly on terrestrial bases or on airborne units can be utilized both for dazzling sensors or blinding optical components, and for kinetic attacks like burning holes on the shells of satellites. Likewise, satellites capable of intercepting a missile are capable of attacking another satellite.[47]

These counterspace capabilities can be organized into an escalation ladder – similarly to the crisis escalation models in other domains.[48] The higher an assault is ranked, the more serious consequences it carries, and therefore the more crucial the deterrence of their attack is.[49]

1. Reversible actions
    1. Electronic and cyber interferences with services – jamming, spoofing, meaconing
    2. Electronic and cyber interferences with components of satellites – dazzling
2. Irreversible actions without environmental degradation
    1. Directed energy and microwave attacks
3. Irreversible actions with environmental degradation
    1. Rendezvous&proximity operations for satellite interception and diversion
    2. Direct-ascent weapons, missile attack on satellites, exploding space mines

[41] They will be detailed in chapter 4.
[42] Horváth, "Countering the counterspace," 93.
[43] Intertanko. *Jamming and Spoofing.*
[44] Mueller, "The Absolute Weapon," 45.
[45] Jones, "China's Shijian-21."
[46] Gouveia, "An Assessment of Anti-Satellite Capabilities," 166.
[47] Wright, The Physics of Space Security, 10.
[48] The original model constructed by Herman Kahn offered a cheat-sheet for decision makers on the process and interdependencies of crisis escalation. Kahn, "On Escalation."
[49] Kopeć, "Space deterrence," 126.

2.2. Selecting cases for analysis

These threats indiscriminately undermine the security of all assets in the orbit, however, until a different extent. While certain types of space capabilities are more resilient or better protected against attacks, others are completely exposed to malicious actions. Therefore, the security of terrestrial bases, weather satellites and satellites of scientific use, satellite early warning systems, positioning, navigation, and timing satellites, communication satellites of civil and military use, intelligence, surveillance, and reconnaissance capabilities, and ASATs will be assessed respectively.

Terrestrial bases – permanent headquarters or mobilized field stations – play an indivisible role in ensuring the undisturbed operation of satellites. Their infrastructure is divided into control stations, data links, processing units, and distribution networks. While smaller ground components can be established on larger ships or even on board of military planes, they are mostly located on the territory of the owner or a friendly host state.[50] This position makes ground units fortified by the protection of the given state's sovereignty as any attack on them would certainly trigger either an act of self-defense under Article 51 of the Charter of the United Nations[51] or a collective response from the Alliance under Article 5 of the Washington Treaty.[52] In addition to the assured deterrence by punishment, achieving benefits by attacking ground stations can be effectively denied by the establishment of a resilient network of bases, as satellites can communicate with several terrestrial units at the same time.[53] Moreover, the fact that space assets can function for longer periods without terrestrial support indicates that an attacker could not gain substantial strategic value from paralyzing the non-kinetic components of terrestrial units either.[54] Thus, bases located on the ground tend to be little payoff targets due to the applicability of deterrence by punishment and deterrence by denial.

Weather satellites and satellites of scientific use bring relatively small contributions to military activities, therefore no aggressor can reape significant strategic benefits by assaulting them. While weather satellites operate in a globally dispersed network mainly in the Geostationary Earth Orbit (GEO) leading to a relatively easy replacement of assets,[55] scientific satellites[56] usually host several nations for space exploration and observation, physical and biological experiments in the Low Earth Orbit (LEO) and Medium Earth Orbit (MEO).[57] Defense capabilities against potential reversible or kinetic attacks were not incorporated into their designs since denying benefits by deploying escort satellites or on-board defense systems would either impose huge financial burden on the nations sponsoring these missions or increase the fuel consumption of the objects resulting in shorter orbital lifetime. However, the exclusively peaceful use of weather satellites, and the involvement of several nations in scientific assets coming with an instant international escalation makes it unlikely that any actor would seriously consider attacking them.

Satellite early warning systems (SEWS)[58] are responsible for surveilling and warning against ballistic and nuclear missile launches. The space components consisting of several early warning radars constitute the heart of launch-on-warning deterrence posture.[59] For this reason, any reversible or damaging attack on these

[50] Ukommi, "Ground Station Design," 12.
[51] A more detailed note on the applicability of self-defence in space by Sulyok, Világűr és Önvédelem.; United Nations, *United Nations Charter*, Art. 51.
[52] NATO, *The North Atlantic Treaty*, Art. 5.
[53] Wright, The Physics of Space Security, 114.
[54] Morgan, *Deterrence and First-Strike*.
[55] Due to gravity wells the effort necessary for launch and placement into orbit should be considered when calculating replacement instead of distance from the Earth's surface. The heavier the object, the deeper is the well, hence the more effort is needed to launch it. Svoboda, "The application of offensive realism," 17.
[56] small artificial satellites, telescopes or crewed megaconstellations.
[57] Van Allen, *Scientific Uses of Earth Satellites*, 1-2.
[58] The last of the 6 satellites of the United States' Space Based Infrared System (changing the earlier Defense Support System satellites in the summer of 2023) has been successfully launched and started its testing phase as of 1st August, 2022. Luckenbaugh, "Final Satellite in Missile Warning System."
[59] Nuclear and Intercontinental Ballistic Missiles are ready to be launched upon warning of an incoming missile, thus, they engage into a retaliation before the attacking missile hits its target. Fetter, "Nuclear Modernization." To

assets bears the risk of a triggering an immediate response. The enormous strategic value of these few satellites coupled with the potential of a nuclear second-strike renders deterrence by punishment highly credible and capable of protecting SEWS capabilities. Deterrence by denial, on the other hand, would not be able to change the cost-benefit calculation of an adversary as these high strategic value assets are low-density and hardly replaceable; without the threat of retaliation they could seem lucrative targets.

Positioning, navigation, and timing (PNT) data services, like the Global Navigation Satellite Systems[60] supply data to civil navigation and aviation, a wide range of military operations and technologies – including Unmanned Aerial Vehicles and precision-guided missiles – transit and transport services, law enforcement, financial sector, and telecommunications. As PNT satellites tend to be high-value but also high-density assets, the physical destruction of individual properties yields no additional gains for the adversary than temporarily disabling their services. Moreover, restricting the operational benefits they provide to NATO nations[61] bears less risk of retaliation than the destruction of a satellite as the causes of non-functioning can be various and hardly attributed. Thus, deterrence by punishment is insufficient to increase the security of PNT satellites. And while their deployment to MEO makes them harder to target than satellites orbiting in the LEO,[62] their downlinks are particularly vulnerable to jamming, spoofing, and meaconing. Although proposals exist for mitigating the exposure to these obtrusions, they cannot retrospectively fit into orbiting devices only a new generation of PNT satellites could accommodate them.[63] Thus, as neither deterrence by denial nor deterrence by punishment offers protection against reversible attacks, PNT assets remain exposed to them.

Commercial satellite communication (SATCOM) stations host a number of international channels and operate through a worldwide dispersed network. They serve several civilian activities ranging from business services, multimedia transmission, network sharing and occasionally contribute to military operations. Despite this dual-use nature, individual assets of the interlinked communication network are considered quite easily replaceable (service-wise) and low strategic value. For this reason, although the resilience of these broadcasters against non-destructive interferences is low, losing an individual asset's data transferring capability would cause no significant disturbance to the service due to the high density of assets. Moreover, satellite antennas can be easily deployed on the board of airplanes and unmanned aerial vehicles. "satellite antennas and dishes can be embedded on airplanes, UAV, vehicles, or even as manpacks".[64] Thus, deterrence by denial through the resiliency of the SATCOM network is apt for guaranteeing the continuity of the service – which in this case overrides the importance of the individual satellite's security – while due to the redundancy of single assets deterrence by punishment cannot credibly deter threats.

Military satellite communication (MILSATCOM) is providing data for NATO's ocean surveillance, communication and control, and reconnaissance, and is more prepared for securing classified information transmission and critical communication in a degraded environment. As the temporary or permanent loss of one or more of these low-density capabilities could cause serious disruption to Allied operations across several domains, these high-value assets are often hardened against nuclear attacks, protected against cyber interferences, and equipped with anti-jamming capabilities.[65] These attempts for deterrence by denial, however, easily fall short of successfully altering the enemy's anticipation of attainable gains. Should an attack succeed in destroying service units, the replacement of a MILSATCOM satellite would be a costly

limit the chances of accidental war, a launch-under-attack approach has been proposed. Marsh, "The probability of accidental nuclear war." 70.

[60] Like the American Global Positioning System, the Russian Global Navigation Satellite System. The European Union, China, India, and Japan also operate regional systems. United Nations Office for Outer Space Affairs, "Global Navigation Satellite Systems."

[61] PNTs are key to command and control, blue-force tracking, missile detection, and battlefield positioning required for precise targeting. Filler et al. *Positioning, navigation and timing.*

[62] Federman, "What Are LEO Satellites."

[63] Jean-Christophe and Frederic, "Positioning, Navigation, and Timing," 623-624.

[64] Tillier, "Telecommunications for Defense," 582.

[65] Tillier, "Telecommunications for Defense," 584-585.

and slow process. Thus, the threat of reprisal against potential attackers enjoys more credibility – particularly since the reliance on MILSATCOM assets is one of the least asymmetric amongst spacefaring nations.

Similarly, intelligence, surveillance, and reconnaissance (ISR) are composed of a few, highly-valuable satellites, which can provide optical imaging for civilian use[66] and military purposes.[67] These services supply valuable information for economic planning, emergency plan execution, and the implementation of military operations.[68] ISR assets are limited in number and are often positioned to one of the Lagrange points to provide regular updates,[69] thus, these high-value assets are easy to target and hard to defend. Making these satellites smaller, more dispersed, or maneuverable would provide a small increase in deterrence by denial's chance to protect assets. However, the degradation of the size would likely come with the degradation of service. Similarly, increasing maneuverability would require adding thrusters to the body of the satellite causing a spike in the cost of launching and operating.[70] But even with thrusters, the number and scale of changes in magnitude or in the velocity direction would remain limited and constrained while adversaries can strike without these limitations.[71] At the same time deterrence by punishment would be no panacea either as assets remain exposed to reversible threats like blinding, dazzling, and jamming.

While most spacefaring nations possess any or every capabilities of the aforementioned space systems, ASAT capabilities stand out as only the United States, Russia, China, and India have demonstrated counterspace capabilities with tests.[72] Thus, ASATs are highly valuable but scarcely present on ground or in orbit, which makes them potentially lucrative strategic targets. Moreover, "the practical lack of defense capabilities means that the adversary will choose a preventive attack on ASAT systems instead of defense."[73] As assets are unlikely to survive a kinetic assault, adversaries are incentivized to resort to non-reversible attacks to destroy others' offensive capabilities before they could be used. Furthermore, the announcement of the Unites States' unilateral restraint on ASAT testing eliminates the option for replacing destroyed counterspace capabilities.[74] Consequently, it is unlikely that denying benefits of destroying the already developed ASATs would deter adversaries from targeting these offensive capabilities. This scarcity and the strategic value, however, lend sufficient credibility for deterrence by punishment against kinetic attacks.

2.3. Implications of the case selection

The assessed categories of satellites highlighted the following results:

Table 1: applicability of deterrence approaches to categories of space assets in case of non-reversible attacks

Category	Deterrence by punishment	Deterrence by denial
Terrestrial base	X	X
Weather & scientific satellite		X
SEWS	X	

[66] Such as fishery, natural hazard forecasts, agricultural insights.
[67] Like electronic and radar surveillance.
[68] Crothers et al. "US Space-based Intelligence."
[69] Due to the increased stability of the orbit caused by the gravity of two celestial bodies these points allow satellites to remain at the same point above the Earth without burning fuel. Starling, *The Future of Security*, 11.
[70] Mueller, *The absolute weapon*, 46.
[71] Wright, The Physics of Space Security, 49.
[72] Currently Australia, France, Iran, Japan, North Korea, South Korea, and the United Kingdom are pursuing programs dedicated to ASAT development. Weeden and Samson, *Global Counterspace Capabilities.*
[73] Kopeć, "Space Deterrence: In Search," 125.
[74] Kimball, "U.S. Commits to ASAT Ban."

Category	Deterrence by punishment	Deterrence by denial
PNT		
SATCOM		X
MILSATCOM	X	
ISR	X	
ASAT	X	

As highlighted by Table 1, the security of PNT satellites was the only category where neither deterrence by punishment nor deterrence by denial is expected to successfully alter the adversary's anticipated cost-benefit calculation. Moreover, no approach was adept for countering reversible interferences mainly due to the lack of reliable attribution. This finding is in line with Lewis' observation that "nondestructive or reversible "attacks" cannot be deterred in peacetime."[75]

Deterrence by denial only showed to be prospective in cases of assets with low strategic value. This resonates with Lewis' observation that "resiliency at the space system (i.e., satellite) level is probably not something that will contribute much at the NATO level of deterrence messaging."[76] However, this implies that an attack against weather & scientific satellites or SATCOM assets is unlikely due to the lack of incentives rather than due to the altered cost-benefit perception. Without the enemy's willingness to carry out an assault, the ability to apply deterrence by denial cannot be verified.[77] This contradicts the findings of Gouveia who emphasized denial as the only effective safeguard against ASAT weapons.[78] Consequently, only deterrence by punishment was confirmed to increase the security of some space asset categories. However, terrestrial bases and SEWS satellites from exceptions from the applicability of space deterrence as the former are protected by conventional deterrence, and the latter by nuclear deterrence. Thus, space deterrence was only proven to be applicable in cases of MILSATCOM, ISR, and ASAT.

These findings confirmed the first hypothesis that deterrence by punishment can be credibly applied in the outer space under certain conditions, while rejected the second and third hypotheses; that deterrence by denial can be credibly applied in the outer space under certain conditions. In line with these results, NATO's assumption on deterrence's credible applicability in space has been confirmed. As a consequence, further analysis is required to establish the variables or conjunctions of variables sufficient for the credible application of deterrence by punishment and the conditions allowing for credible threats in space.

2.4. What makes space assets defensible by deterrence by punishment?

The theoretical confirmation of deterrence's credible applicability in outer space alone is not sufficient to answer whether NATO can implement deterrence in space. Determining the common variables and conditions that enable the credible application of deterrence by punishment are precondition for identifying gaps that improved SSA could fill in.

2.4.1. Conjunction of variables

Based on the theoretical review of the dominant approaches of deterrence, deterrence by punishment requires the enemy to believe that the cost of reprisal after an attack would exceed the benefits obtained by the

[75] Lewis, "Reconsidering Deterrence," 61.
[76] Lewis, "The Increasing Importance," 12.
[77] Quackenbush, "Identifying opportunity for conflict," 37-38.
[78] Gouveia, "An Assessment," 171.

assault. Although the aim of deterrence is to provide protection without launching an attack, the deterring effect only remains viable until the adversary knows that NATO is determined to launch a retaliatory attack. For this credibility the adversary needs to perceive that an attack would leave no chance for the Alliance but reprisal.

During the case selection four ordinal variables could be identified to play a role in the applicability of deterrence approaches. The strategic value of an asset perceived by the adversary, the replaceability of the degraded service or unit, the resilience of the spacecrafts against external electronic, cyber, and kinetic interferences,[79] and the dispersion of the satellite configuration values were identified with values of high (H) or low (L).

Table 2: common set of variables of assets protected by deterrence by punishment

Category	Strategic value	Replaceability	Resilience		Density
			Reversible	Non-reversible	
MILSATCOM	H	L	H	L	L
ISR	H	L	L	L	L
ASAT	H	L	L	L	L

As shown, the conjunctions of high strategic value, low replaceability, low resilience, and low density variables are sufficient for the credible application of deterrence by punishment in space. These findings are in line with the theoretical expectations and highlight the features NATO should seek in MILSATCOM, ISR, and ASAT capabilities to implement deterrence credibly in the outer space domain.[80] However, not even the presence of the conjunction of variables will leave the Alliance with unrestrained options to utilize the threats of punishment. The following section will provide an overview of the reprisals fitting to the outer space's operational constraints.

2.4.2. Conditions for credible punishments

The unique physical features of the fifth operational domain impose limitations on the threats of punishment NATO can credibly signal to its adversaries. Harrison identified three central issues restricting deterrence by punishment in space; the "vulnerability gap", the credibility of carrying out a threat in an asymmetric environment, and the weakness of space situational awareness.[81]

The first issue concerns the symmetric responses NATO can give to a non-reversible assault on its space assets. Such a tit-for-tat – a counterattack corresponding to the adversary's attack to cause roughly corresponding loss to the caused damage – would be hindered by the fact that NATO lacks the "escalation dominance" as the organization would run out of enemy satellite targets even if it choose to retaliate.[82] Moreover, as Harrison observed, the vulnerability gap leads the adversary to the perception that even if

[79] Resilience includes the robustness of the system, the ability to recover service after a reversible attack, and the feasibility of reconstitution of the asset after a kinetic attack. Burch, "A Method for Calculation," 1002.
[80] Although each cost-benefit calculation is subject to the perception of the aggressor in that specific scenario, and therefore any conclusion is limited to the specific circumstances and the respective type of asset, the similarity of vulnerabilities of the studied assets allows for some general findings.
[81] Harrison et al, "Space deterrence," 10.
[82] Koplow, "Deterrence as the MacGuffin," 336.

NATO attributed the perpetrator and responded in kind, the Alliance would suffer disproportionate degradation in space services. [83]

The unbalanced exposure of NATO asset also implies that the Alliance is more interested in the preservation of the operational environment than its adversaries. Consequently, while kinetic damages, degrading components, or destruction of the whole space object would justify a more costly retribution to the enemy, only attacks that do not generate space debris can be taken into account. As such, the issue of orbital debris creation has been on the forefront of space security policies for decades now. The increasing fear of reaching the "cascade effect" – the uncontrollable and self-generating collision of space debris with other space objects leaving the environment even more degraded – has been widely voiced by experts.[84] Any attack resulting collateral damage or the physical destruction of space would take another step towards the loss of swathes of usable orbits, and thereby lead to a self-defeating result in addition to the international condemnation. This undermines NATO's threats to use kinetic force as "there needs to be a belief that the political will exists to respond with severe military response if attacked."[85] Consequently, the credibility of carrying out a threat in an asymmetric environment is limited to non-destructive reprisals. These, however, are not limited to counterattacks within the space domain since according to International Law, reprisals must be proportionate but not necessarily symmetric.[86] Nevertheless, cross-domain responses need to observe proportionality and preferably remain in a logical connection to the attack. The threat of bombing cities for an annihilated satellite would not only eliminate the threat's credibility but would also seem escalatory regardless of the mutual violation of sovereignty. Thus, even a reprisal in the time, domain, and quality of NATO's choice faces limitations.[87]

Even with the invitation of other domains into space deterrence, the third issue, attribution remains unresolved. As the identification of perpetrators is limited – especially in cases of reversible attacks – non-kinetic assaults offer a good cost-benefit value for adversaries. While they can significantly degrade NATO's capability to respond to any crisis, use precision-guided weapons, or conduct effective secret communication, risk of a seriously damaging retribution is relatively low. Moreover, attacks on ISR, PNT, and MILSATCOM capabilities can further limit NATO's rapid and prompt responses.

3. A MOMENTUM FOR SPACE SITUATIONAL AWARENESS

3.1. Potentials for an improved SSA

While SSA is composed of three elements; space weather, natural space debris, and orbiting space objects – the first two being indispensable for space safety – this paper only concerns security, and remarks will henceforth only regard the third one. Thus, the development of SSA entails more precise tracking of resident space objects and their anticipated behavior.

As the analysis proved, NATO's ability to deter reversible threats is not in close range yet, therefore this section will only seek to explore deterrence against non-reversible threats. One of the gaps identified by Harrison, the weakness of SSA provides room for believing that even if other variables remain constant, the improvement of SSA correlates with an hightened scope of deterrence.

Broadening this scope can evolve along multiple tracks. In the realm of deterrence by punishment SSA can either deepen the credibility of already applicable deterrence, or broaden it by applying itt o additional assets. In case of deterrence by denial the proof that the strategy is able to guarantee the security of any space capability would be considered as a broadening.

[83] Harrison, "The Role of Space," 115.
[84] Imburgia, "Space debris," 597., Mejía-Kaiser, "Space Debris Mitigation."
[85] Klein, Understanding space strategy, 73.
[86] Stephens and Steer, "Conflicts in space," 40.
[87] Paulauskas, "Space: NATO's latest frontier."

3.1.1. SSA and deterrence by punishment in space

Improving SSA bears important operational ramifications for deterrence by punishment as it enables a more nuanced threat assessment. The implications of benefits obtained by this enhanced information on the state of the affairs are threefold. First, the increased ability to assess the seriousness of the threat allows NATO to respond to it with a proportionate counterthreat. Thus, the more precisely eseteemed corcumstances lead to more credible communication and prevent the Alliance from being perceived as an agressor. Second, the ability to predict the behavior (and constraints) of space assets will significantly improve attribution. This implies that perpetrators will have a lower chance to shirk responsibility and hide behind anonimity. In light of a certain retaliation the cost-benefit calculation of the adversary cannot remain unconstrained, theferore adversaries will be more likely to refrain from resorting to the use of force against NATO. Third, mergining national SSA information through data repositories will allow an even greater accuracy of locating targets. This provides a greater room for using precision-guided weapons in space while also limits the fear over generating space debris by imprecise strikes. Thus, improved SSA will undoubtly contribute to the deepening of deterrence by punishment in space.

The question of broadening the scope of deterrence by punishment through guaranteeing the security of additional assets is only relevant for one type of capability; PNT. While other assets were demonstratedly protected by deterrence by punishment or remained outside of the strategic interests of adversaries, none of the approaches were able to provide for the security of PNTs. Considering the conjunction of sufficient variables, PNTs are only diverging in their density from ISR, MILSATCOM, and ASAT capabilities. However, the reason of deterrence by punishment failing to deter attacks on PNTs is not caused by this difference. As the analysis highlighted, agressors are more motivated to rely on reversible attacks against PNT assets than on kinetic assaults as they yield the same benefits with lower risks. However, as the case studies underlined, currently deterrence fails against reversible threats. Thus, SSA is not to be blamed for its inability to widen the applicability of deterrence by punishment to PNTs.

3.1.2. SSA and deterrence by denial in space

The potential for deterrence by denial was only proven in cases of assets with low strategic value, high replaceability, high resilience, and high density. However, due to their limited or no contribution to military operations these assets usually fall outside of the interests of adversaries. Theoretically improved SSA could enable the applicability of deterrence by denial as it would lead to the limitation of surprise attacks and an enhanced damage assessment. However, increasing resilience of assets not in the way of harm would not make the concept of deterrence by denial any more applicable.

Therefore, it is more prospective to examine the opportunities of deterrence by denial for the only type of asset not protected otherwise, PNT satellites. The question whether the exposure of PNT capabilities to reversible attacks would be limited by their increased resilience is a prospective subject for further inquiries. If such a shift would occur, enhanced SSA could rightfully claim the credit for extending the scope of deterrence by denial's credible applicability in space.

4. CONCLUSION

This paper intended to provide an answer to whether improved Space Situational Awareness (SSA) can broaden the scope of space deterrence's credible applicability. For that the first part of the analysis established – in line with the first hypothesis – that NATO can only implement deterrence credibly in outer space by utilizing deterrence by punishment. Moreover, limitations of this strategy has also been introduced through a conjunction of variables and certain conditions.

The second part undertook the initiative to adress the gaps identified during the first round of analysis by exploring the opportunities SSA development can present. The improvement of SSA proved to be able to

deepen the scope of deterrence by punsihment and provided hope for the applicability of deterrence by denial for PNT capabilities. Thus, the Space Situational Awareness System's development[88] is likely to ease NATO's Space Deterrence Dilemma.

[88] NATO, "NATO and Luxembourg."