Original Study **Open Access**

Alper Ören*

Rethinking strategic stability in space through technologically dynamic deterrence model

DOI 10.2478/jms-2025-0006
Received: May 19, 2025; Accepted: August 24, 2025

Abstract: As outer space emerges as a central domain of geopolitical contestation and technological disruption, the conceptual tools of classical deterrence are proving increasingly inadequate. Traditional models, grounded in nuclear-era assumptions of rational actors, dyadic competition and visible escalation thresholds, fail to capture the complexity of today's contested orbital environment. This article addresses this theoretical shortfall by proposing a conceptually and operationally innovative deterrence architecture: Technologically dynamic deterrence model (TDDM). Integrating insights from strategic theory, space security and emerging technology studies, TDDM reconceptualises deterrence as a layered, adaptive and metrics-driven system tailored to the realities of the contemporary space domain. Through comparative analysis of U.S., Chinese and NATO space strategies, the article demonstrates the divergent logics of modern deterrence postures and highlights the growing risks of doctrinal misalignment and normative fragmentation. It concludes by offering a set of policy recommendations aimed at enhancing strategic stability through resilience, transparency and cross-domain integration. The study contributes to both theoretical innovation and practical guidance, offering a comprehensive pathway for deterrence thinking in the era of space militarisation and emerging technologies.

Keywords: space deterrence, emerging and disruptive technologies, space security, deterrence theory, space governance

Abbreviations: A2/AD, anti-access/area denial; ABM, anti-ballistic missile; ASAT, anti-satellite weapons; C4ISR, command, control, communications, computers, intelligence, surveillance and reconnaissance; CBES, confidence-building engagement score; EDT, emerging and disruptive technology; EER, escalation elasticity ratio; ESA, European space agency; GEO, geostationary orbit; INF, intermediate nuclear forces; IRIS², infrastructure for resilience, interconnectivity and security by satellite; KPIs, key performance indicators; LEO, low earth orbit; MAD, mutual assured destruction; MEO, medium earth orbit; MLD, multi-layered deterrence; MTP, minimum transparency protocol; NPT, treaty on the non-proliferation of nuclear; OST, outer space treaty; PWSA, proliferated warfighter space architecture; RRM, resilience readiness metric; SAI, strategic ambiguity index; SALT, strategic arms limitation talks; SSA, space situational awareness; SSSD, space strategic stability dialogue; START, strategic arms reduction treaty; STM, space traffic management; STO, science & technology organisation; TDDM, technologically dynamic deterrence model; TDSR, tech-doctrine synchronisation rate; UNOOSA, United Nations Office for Outer Space Affairs; WMD, weapons of mass destruction.

1 Introduction

The strategic landscape of outer space is undergoing a profound transformation. Once perceived as a domain reserved for scientific exploration and peaceful cooperation, space has evolved into a critical arena of geopolitical contestation and technological rivalry (Elefteriu 2024). This transformation is driven not only by the increasing militarisation of space but also by the rapid proliferation of emerging and disruptive technologies (EDTs) that challenge the very foundations of traditional deterrence theory and international stability (Harrison et al. 2021).

From the deployment of mega-constellations to the testing of kinetic and non-kinetic anti-satellite weapons (ASAT), contemporary space dynamics illustrate a shift from a predictable, bipolar order toward a multipolar and asymmetric environment (Garretson 2021) marked

***Corresponding author: Alper Ören,** PhD Alumni, Eskisehir Technical University Department of Aerospace and Aeronautics, 26555, Eskişehir, Türkiye, E-mail: alper.oren@outlook.com

by dual-use ambiguity, private sector proliferation and technological leapfrogging. SpaceX's Starlink, China's Shijian satellite series (Wang et al. 2024) and the U.S. Department of Defense's Proliferated Warfighter Space Architecture (PWSA) (Berglund 2024) exemplify how both state and commercial actors now shape the strategic calculus in orbit. In parallel, counterspace capabilities – including co-orbital systems, directed energy weapons, jammers and cyber tools – are no longer hypothetical threats (Samson 2024) but tangible realities, integrated into national security doctrines and tested in increasingly sophisticated ways.

At the core of this evolving environment lies a critical question: Can existing deterrence theories, rooted in Cold War-era nuclear paradigms, adequately capture the complexity and fluidity of the contemporary space domain? The answer, this article contends, is increasingly negative. Space deterrence is no longer confined to doctrines of denial and punishment (Rice 2023); it must now grapple with questions of resilience, attribution, strategic ambiguity and the proliferation of autonomous systems. The traditional rational actor model struggles to remain relevant in a setting where machine-speed decision-making, algorithmic warfare and the opacity of private-sector infrastructure introduce new escalation pathways and deterrence dilemmas.

Complicating matters further is the pace and scope of technological disruption. Artificial intelligence (AI), quantum communications, software-defined satellites and additive manufacturing are not merely enhancing existing systems – they are redefining what is strategically possible. The McKinsey Technology Trends Outlook (Yee et al. 2024) notes the accelerating integration of generative AI and autonomous robotics into critical infrastructure, including space systems. Meanwhile, the Secure World Foundation's 2024 Counterspace Capabilities Report details the growing sophistication of reversible and non-reversible interference tools across multiple actors, illustrating a crowded and contested domain with minimal normative clarity.

This article aims to contribute a novel conceptual framework that addresses this epistemological gap. It proposes a reconfiguration of space deterrence theory – one that recognises the role of technological acceleration, dual-use ambiguity and the multiplicity of actors in shaping deterrence effectiveness. Furthermore, it introduces Key Performance Indicators (KPIs) for evaluating deterrence outcomes in the space domain, grounded in both empirical case studies and theoretical reflection. Drawing on recent satellite interference incidents, doctrinal developments and strategic communications, this framework seeks to provide scholars and policymakers with a more adaptive and forward-looking toolkit for managing the risks of escalation and ensuring strategic stability in space.

In doing so, the article takes seriously the proposition that space is not merely a reflection of terrestrial power politics but a unique arena with its own strategic logic – one that requires equally unique approaches to deterrence, governance and conflict prevention. As outer space continues to converge with terrestrial conflict dynamics, particularly through hybrid and grey-zone operations, the urgency of updating our conceptual and policy architectures becomes ever more critical (Dugger 2025).

2 The limitations of classical deterrence theories in the space domain

Deterrence theory, as classically understood, emerged during the nuclear standoff of the Cold War – a period characterised by strategic dyads, central state authority and the assumption of rationality among actors. These early formulations, rooted in the works of Schelling (1966); Jervis (1976), and Waltz (1979), emphasised notions such as mutual assured destruction (MAD) (Jervis 2002), 'Second-Strike Credibility' (Long and Green 2015) and 'Deterrence by Punishment or Denial' (Pape 1992). While these paradigms provided clarity in a bipolar, terrestrial and nuclear context, their assumptions falter when applied to the contemporary space environment.

Space deterrence presents at least five fundamental challenges to classical deterrence theory:

2.1 Multipolarity and actor diversity

The outer space domain is no longer the exclusive purview of a few great powers. Over 90 countries operate satellites, and more than 70 private companies maintain orbital infrastructure, according to the 2024 State of Satellite Deployments report (Slingshot Aerospace 2024). This diversity undermines the dyadic structure that classical deterrence theory relies on. Moreover, the entry of non-state actors and commercial actors with strategic relevance (e.g., Starlink's role in Ukraine) introduces

unpredictability and complicates the attribution essential for deterrence to function.

2.2 Dual-use ambiguity and intent uncertainty

In space, many systems serve both civilian and military functions – a satellite may simultaneously support commercial communications, military reconnaissance and navigation (Vlasic 1991). This dual-use ambiguity (Pražák 2021) blurs the distinction between legitimate targets and acts of aggression, challenging the assumptions of clarity and signalling embedded in deterrence logic (New Space Economy 2025). As noted in the Space Threat Assessment (Swope et al. 2024), the indistinguishability between a servicing satellite and a co-orbital ASAT system exemplifies this dilemma.

2.3 Non-kinetic and reversible counterspace capabilities

Traditional deterrence relies on the threat of punishment through highly destructive means (Kahan 1999). Yet many contemporary counterspace threats – such as cyberattacks, jamming, spoofing and dazzling – are non-kinetic, reversible and often deniable. These features lower the threshold for use and increase the challenge of attribution, undermining the escalatory clarity needed for deterrence to hold. As the Secure World Foundation's 2024 Counterspace Capabilities Report illustrates, states are increasingly investing in capabilities designed to operate below the threshold of armed conflict – a domain in which classical models offer limited predictive power.

2.4 The speed of EDTs-driven conflict

Emerging technologies – especially AI, machine-speed decision systems and autonomous spacecraft – drastically compress the decision-making window (Lucarelli et al. 2021). In classical theory, deterrence was predicated on deliberation, signalling and strategic calculus (Coletta 2023); in contrast, modern engagements may unfold at speeds that render traditional crisis management tools obsolete. A satellite-disabling event triggered by an AI-driven threat assessment algorithm may escalate faster than humans can respond or interpret, raising questions about the reliability of deterrence through rationality.

2.5 Absence of norms and arms control regimes

Unlike nuclear deterrence, which evolved alongside treaties such as strategic arms reduction treaty (START), treaty on the non-proliferation of nuclear (NPT) and intermediate nuclear forces (INF), space deterrence operates in a largely ungoverned strategic domain (Lambakis 2022), relative to other domains such as nuclear or cyber. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (a.k.a OST – outer space treaty) prohibits the placement of weapons of mass destruction (WMD) in orbit but offers little guidance on conventional or non-kinetic counterspace capabilities. The absence of binding norms and confidence-building measures contributes to strategic opacity, arms racing and norm erosion, further weakening the classical deterrence framework (Hersman et al. 2022). The 2022 The Geneva Centre for Security Policy report on 'Preventing Increased Militarisation of Outer Space' (Al-Rodhan 2023) emphasises the urgent need for preventive diplomacy and norm entrepreneurship.

In sum, while deterrence remains a relevant strategic concept, its classical formulations must be reconceptualised to address the realities of technologically fluid, actor-dense and strategically ambiguous outer space operations. The next section of this article will therefore propose a novel framework for space deterrence, rooted in adaptability, technological foresight and empirically grounded performance metrics. This approach seeks to offer scholars and practitioners an actionable model better suited to the multi-domain, high-velocity nature of contemporary space competition.

2.6 Reframing deterrence: comparing classical and space-specific paradigms

The intellectual foundations of deterrence theory, developed during the Cold War, rest upon a set of stable assumptions concerning the nature of conflict, actors, weapons systems and strategic signalling (Gartzke and Lindsay 2024). These assumptions, however, are increasingly misaligned with the realities of the modern space domain.

Table 1 presents a structured comparison between classical deterrence theory, rooted in Cold War-era strategic thinking, and the emerging logic of space deterrence, shaped by contemporary geopolitical, technological and normative dynamics. Each dimension captures a critical point of divergence, illustrating why conventional

Tab. 1: Core structural contrasts between classical and space deterrence

Dimension	Classical deterrence	Contemporary space deterrence
Strategic domain	Terrestrial (mainly land and sea)	Multi-orbit space (LEO, MEO, GEO, cislunar)
Actor structure	Bipolar, state-centric	Multipolar, including commercial actors
Weapons type	Kinetic, high-yield	Reversible, non-kinetic, dual-use
Escalation thresholds	High and visible	Low and ambiguous
Attribution	Generally clear	Often uncertain or deniable
Strategic Signalling	Declarative, symbolic (e.g. nuclear tests)	Embedded in orbital behaviour, capability ambiguity
Speed of decision-making	Deliberative, slow	Machine-speed, algorithmic, real-time
Legal framework	Treaty-rich, structured	Fragmented, with large regulatory gaps

GEO, geostationary orbit; LEO, low earth orbit; MEO, medium earth orbit.

deterrence models are insufficient for addressing the distinct challenges of the orbital domain.

2.6.1 Strategic domain

Classical deterrence was conceptualised within terrestrial theatres – land, sea and air – where geography and surveillance defined strategic boundaries. In contrast, space deterrence unfolds across multiple orbital regimes (low earth orbit [LEO], medium earth orbit [MEO], geostationary orbit [GEO], cislunar), each with varying physical constraints, latency factors and monitoring challenges. The lack of natural boundaries and the orbital fluidity of assets create a fundamentally different spatial logic, complicating strategic predictability.

2.6.2 Actor structure

Traditional deterrence theories assumed a bipolar configuration with state actors wielding centralised control over strategic arsenals. The current space environment is multipolar and increasingly hybrid, encompassing state, commercial and consortium-based actors. This proliferation of stakeholders diffuses authority, complicates signalling and introduces asymmetries in capability, intent and accountability.

2.6.3 Weapons type

Classical deterrence relied on large-scale, high-yield kinetic weapons, predominantly nuclear, that provided immediate and irrevocable effects. In the space domain, the dominant tools of coercion are non-kinetic, often reversible and frequently dual-use in nature. Techniques such as cyber interference, jamming and co-orbital shadowing permit coercion without crossing the kinetic threshold, thereby expanding the grey zone of deterrence interaction.

2.6.4 Escalation thresholds

The strategic calculus of the Cold War presumed clearly defined escalation ladders. In space, the boundaries are blurred. The ambiguity surrounding intent, effect attribution and damage reversibility creates low and ambiguous escalation thresholds, raising the risk of inadvertent conflict or disproportionate retaliation.

2.6.5 Attribution

Clear attribution was essential to the logic of mutually assured destruction. In space, attribution is often technically difficult and politically contested. The difficulty in identifying the origin of interference – whether from a state, non-state proxy or environmental factor – undermines the credibility of threat–response cycles and weakens deterrence-by-retaliation models.

2.6.6 Strategic signalling

Historically, deterrence relied on overt and symbolic acts – nuclear tests, military parades and public doctrine releases. In space, signalling occurs through operational behaviour, such as satellite manoeuvring, proximity operations and deployment patterns. These acts are less legible, and without a shared interpretive framework, may increase misperception rather than deter aggression.

2.6.7 Speed of decision-making

The nuclear era allowed for deliberate, often time-intensive decision-making. In contrast, space operations – particularly in LEO – can unfold in minutes or seconds. The introduction of AI-driven space situational awareness (SSA) systems and autonomous platforms accelerates this timeline further, demanding pre-delegated rules of engagement and challenging the role of human judgement in escalation control.

2.6.8 Legal framework

Classical deterrence evolved alongside a robust treaty architecture (e.g., NPT, strategic arms limitation talks [SALT], anti-ballistic missile [ABM] treaty), which provided both behavioural expectations and enforcement mechanisms. Space governance, however, remains fragmented and largely symbolic, anchored in legacy agreements such as the 1967 OST, which lack provisions for enforcement, counterspace activity regulation, or conflict mitigation. This legal vacuum introduces structural instability into the deterrence equation.

In sum, Table 1 illustrates that space deterrence is not merely an extension of terrestrial deterrence into a new domain; it is a distinct strategic construct, requiring new theories, adaptive doctrines and domain-specific tools. Recognising these structural differences is foundational for the development of contemporary deterrence models such as the technologically dynamic deterrence model (TDDM), which this article advances in subsequent sections.

2.6.9 Analytical commentary on the comparison

2.6.9.1 Domain shift and multi-orbital complexity

Whereas classical deterrence was situated in well-mapped terrestrial environments, space deterrence operates across multiple orbital regimes with vastly different surveillance, manoeuvrability and latency characteristics (Farrell 2024). Deterrence logic in LEO, where close approaches can happen within minutes, cannot be uniformly applied to GEO or emerging cislunar theatres (Svoboda 2022), which feature extended timelines and sparse c coverage. This orbital diversity undermines the spatial predictability that underpinned Cold War-era deterrence strategies.

2.6.9.2 From Bipolarity to Multipolar Complexity

Classical deterrence theory was built for bipolar rivalry between superpowers with symmetrical capabilities and centralised control (Tunsjø 2022). Today's space deterrence environment includes dozens of state actors, private satellite operators and international consortia (Flanagan et al. 2023). The participation of companies like SpaceX, OneWeb and Blue Origin, alongside state-aligned private firms in China, introduces fragmentation and unpredictability. The traditional assumption of unitary, rational actors – central to Schelling's theory of deterrence (Schelling 1962) – is no longer tenable.

2.6.9.3 Weapon typology and reversibility

Nuclear weapons provided the archetype for deterrence by punishment, based on their immediate and irreversible destructive capacity (Mazarr 2018). In contrast, most counterspace capabilities today are reversible and non-lethal: cyber intrusions, jamming, laser dazzling and signal spoofing. These tools allow for deniable interference, complicating retaliation thresholds and increasing the strategic tolerance for risk-taking behaviour. This significantly erodes the credibility and clarity of deterrent signalling, a cornerstone of classical frameworks.

2.6.9.4 Escalation and attribution ambiguities

One of the most profound departures from classical theory is the opacity surrounding attribution in the space domain (Miller 2021). A degraded satellite may result from a technical malfunction, a naturally occurring event (e.g., solar radiation), or a hostile act. Without clear attribution, proportional retaliation becomes politically and strategically dangerous, weakening deterrence by punishment. Moreover, escalation pathways in space are non-linear and often invisible, undermining confidence in strategic stability mechanisms.

2.6.9.5 Accelerated decision cycles and strategic speed

In classical deterrence models, states had time for deliberation due to long-range missile trajectories and slow-moving crises (Ghoshal 2023). In contrast, space incidents – especially in LEO – can unfold within minutes or seconds, driven by AI-supported situational awareness tools and autonomous manoeuvring satellites. These compressed timelines reduce the effectiveness of strategic communication and increase the likelihood of inadvertent escalation, particularly when human-in-the-loop systems are bypassed.

2.6.9.6 Legal and normative gaps

Classical deterrence evolved alongside robust legal regimes, such as NPT, SALT, START and confidence-building measures. In contrast, space law remains

anchored in the 1967 OST, which lacks enforcement mechanisms for counterspace conduct and remains silent on emerging technologies. The lack of transparent and enforceable norms creates a deterrence vacuum, increasing the risk of misperception and preemptive actions (Bertolini et al. 2023).

2.6.10 Strategic implication

Table 1 and its analysis highlight the theoretical disconnect between Cold War paradigms and 21st-century deterrence needs in space. This mismatch is not merely academic; it affects real-world policy design, crisis management and escalation control. It justifies the imperative for conceptual renewal, paving the way for the proposed TDDM in the next section. Acknowledging these differences is the first step toward creating a model of deterrence tailored to the domain-specific realities of space – not just inherited from terrestrial analogies.

3 Toward a novel framework for space deterrence in the age of technological disruption

In response to the growing inadequacy of classical deterrence theory when applied to the space domain (Peace 2023), this section introduces a novel, multi-dimensional deterrence framework that is adaptive, layered and technologically integrated. The proposed TDDM is designed to align with the characteristics of the modern space environment: speed, ambiguity, autonomy and asymmetry. It draws on empirical trends, conceptual insights from critical security studies, and foresight derived from technology innovation models.

While the TDDM is primarily a conceptual framework, its scientific validity is grounded in a triangulated methodology combining theoretical synthesis, comparative strategic analysis and foresight-based systems modelling. Rather than relying solely on empirical hypothesis testing, the model draws on a normative-analytical approach widely used in strategic studies, where complex variables, limited data environments and future-oriented scenarios render conventional validation methods insufficient. The argumentation throughout the article is supported by a comparative analysis of U.S., Chinese, and NATO deterrence postures, structured through operational KPIs, which serve as proxy indicators for deterrence logic in a contested orbital environment. By aligning conceptual premises with strategic behaviour and documented counterspace capabilities, the model attains internal consistency, explanatory value and policy relevance – hallmarks of scientific validity in theoretical innovation. Furthermore, the proposed KPIs enable the model to be tested, refined and iteratively calibrated in future studies using simulations, escalation modelling, or scenario-based strategic games, thus laying the foundation for progressive empirical validation.

The methodological approach employed in developing the TDDM is structured around qualitative comparative analysis and theory-informed case study logic. The selection of the United States, China and NATO/European partners as case studies reflects three distinct deterrence paradigms – resilience-first, ambiguity-centric and norm-driven – which collectively offer a comprehensive spectrum of strategic postures in the orbital domain. These actors were also chosen based on the availability of open-source doctrinal materials, strategic policy documents and data on counterspace capabilities. The selection of KPIs was informed by a triangulated process, incorporating insights from strategic theory, systems engineering and recent defence policy literature. Each KPI was designed to correspond to a foundational attribute of deterrence as reconceptualised in the space domain: ambiguity, survivability, doctrinal coherence, escalation elasticity and normative engagement. This methodology ensures that the model remains theoretically robust while maintaining practical relevance for both academic and policy applications.

3.1 Foundational premises of the new model

The TDDM rests on five interlinked premises.

3.1.1 Strategic resilience as a core deterrence attribute

In an environment where attribution is difficult and attacks may be non-lethal yet disruptive, resilience becomes deterrence. The visible capacity to recover, reconfigure, or reroute space assets (e.g., through proliferated LEO constellations or autonomous network patching) serves as a deterrent-by-futility, signalling to adversaries that aggression will not yield strategic advantage (Cavaciuti et al. 2022).

3.1.2 Multi-layered deterrence (MLD) architecture

Deterrence in the space domain must be reconceptualised as a multi-layered construct, in which distinct yet

interdependent dimensions operate in concert to shape adversary behaviour and ensure strategic stability. At the physical layer, deterrence is established through architectural resilience, including spacecraft hardening, orbital manoeuvrability and systemic redundancy – all aimed at denying adversaries the ability to inflict decisive or irreversible damage. The cyber layer involves the deployment of active defence mechanisms, zero-trust architectures and intrusion detection systems that secure critical space infrastructure against digital exploitation and sabotage. The doctrinal layer is expressed through publicly declared red lines, deterrent thresholds and preemptive response postures that shape expectations and constrain adversarial decision-making. Finally, the cognitive layer encompasses strategic signalling, narrative framing and perception management – tools that influence how actions are interpreted, how resolve is perceived and how escalation is calibrated. Taken together, these layers form an integrated deterrence architecture that enhances adaptability, complicates adversary planning and reinforces cross-domain stability in the increasingly complex space environment. This multi-layer model aligns with the complexity revealed in the NATO STO Trends 2023–2043 (NATO Science & Technology Organization 2023), which emphasises cross-domain integration and decision dominance.

3.1.3 Integration of emerging technologies into deterrence signalling

The rise of AI, quantum communications and real-time satellite swarm manoeuvres introduces new signalling mechanisms (Oche et al. 2021). The visibility of these capabilities – such as AI-predicted manoeuvre avoidance, automated coordination with commercial constellations, or quantum-resilient communications – becomes part of a deterrence portfolio. This is not unlike the nuclear submarine patrols of the Cold War – an implicit reminder of strategic capability.

3.1.4 Proactive normative shaping as soft deterrence

Deterrence is not only reactive; it is also proactive (Filippidou 2020). States that lead norm development in space – for example, by promoting transparency in satellite behaviours, publishing responsible counterspace principles, or engaging in confidence-building with rivals – shape adversarial expectations. This is a form of strategic norm entrepreneurship, functioning as deterrence by community anchoring.

3.1.5 KPI-driven strategic evaluation

Drawing from systems engineering and strategic foresight approaches, the model proposes a quantitative performance monitoring tool to assess deterrence health. Suggested KPIs include:

- ***Strategic Ambiguity Index (SAI):*** Measures the degree to which military space assets are indistinguishable from civilian ones – higher values indicate greater escalation risk.
- ***Resilience Readiness Metric (RRM):*** Evaluates the time-to-recovery and autonomy index of space systems post-disruption.
- ***Tech-Doctrine Synchronisation Rate (TDSR):*** Assesses how closely operational doctrines reflect current technological capabilities.
- ***Escalation Elasticity Ratio (EER):*** Gauges how quickly reversible counterspace measures escalate to irreversible actions under various doctrines.
- ***Confidence-Building Engagement Score (CBES):*** Measures the degree to which an actor participates in transparency, dialogue and norm-shaping initiatives in the space domain.

3.2 Illustrative case: deterrence-by-resilience in the Russia–Ukraine conflict

A concrete manifestation of this model emerged in the early stages of the Russia–Ukraine war, where SpaceX's Starlink constellation provided Ukraine with uninterrupted connectivity (Gurantz 2024), despite targeted jamming and cyber interference. Russia's failure to disable the network – largely due to its decentralised, agile infrastructure and rapid software adaptation – served as an implicit deterrence signal. The episode illustrates how resilience, not retaliation, prevented the escalation of counterspace hostilities, and how private-sector capabilities can become embedded in a nation's strategic deterrence posture.

This enhanced model does not seek to replace classical deterrence frameworks outright but to augment them with attributes and metrics suited for a post-linear, multi-domain and tech-intensive space environment. In the following section, the article will explore how this model can be applied to evaluate existing national space strategies and defence doctrines, and how policymakers might calibrate their deterrence postures accordingly.

3.3 Operationalising deterrence: KPIs for the space domain

Deterrence in the space domain requires more than theoretical reframing (Carey and McGillis 2024) – it demands operational metrics capable of capturing the effectiveness, stability and credibility of deterrent postures. The TDDM introduces a novel set of KPIs to serve as diagnostic and strategic tools for policymakers and defence planners. Table 2 introduces a structured set of KPIs that operationalise the abstract principles of deterrence within the complex and dynamic context of outer space. These KPIs reflect the core dimensions of the TDDM and are intended to serve as diagnostic, comparative and adaptive tools for policymakers, defence analysts and strategic planners.

Unlike conventional deterrence frameworks that rely heavily on declaratory posture or kinetic capability, this KPI-based approach enables a quantitative and qualitative assessment of how deterrence is structured, signalled and perceived in space.

The TDDM introduces a performance-based framework for assessing the health, credibility and adaptability of space deterrence postures. Central to this model is a suite of KPIs, each designed to capture a specific dimension of deterrence logic in the orbital domain.

These KPIs include the SAI, which measures the opaqueness of intent and capability in dual-use systems; the RRM, which evaluates system survivability and recovery speed; the TDSR, which identifies alignment between technological adoption and doctrinal integration; the EER, which gauges tolerance to ambiguous disruptions; and the CBES, which assesses an actor's transparency and normative signalling behaviour.

Each of these indicators provides a distinct lens through which deterrence performance can be measured, compared and recalibrated. A more detailed explanation of these KPIs and their strategic utility is provided in the analytical commentary accompanying Table 2.

The SAI captures the degree to which an actor's space capabilities, behaviours and deployments obscure the line between civilian and military intent. In an environment saturated with dual-use satellites and multi-mission platforms, ambiguity can be both a shield and a threat. High ambiguity may deter adversaries through uncertainty but also increases the risk of misinterpretation, escalation or inadvertent targeting. The SAI thus provides a metric for balancing deterrent opacity with signalling clarity.

The RRM evaluates a space system's capacity to absorb disruption and maintain mission continuity. This includes architectural features such as proliferated constellations, autonomous recovery functions, hardened communications and redundancy pathways. High resilience reduces the strategic incentive for attack, reinforcing deterrence-by-denial. The RRM is particularly valuable in measuring non-escalatory deterrence, where survivability replaces retaliation as the dominant strategic message.

The TDSR assesses the alignment between an actor's technological capabilities and its strategic doctrine or operational concept. In rapidly evolving space technology environments, there is often a temporal lag between capability acquisition and doctrinal adaptation. A low TDSR indicates a risk of underutilised assets or reactive postures, while a high TDSR reflects doctrinal agility and the capacity to strategically integrate new technologies – such as AI, cyber tools, or quantum communications – into deterrence planning.

The EER measures the threshold sensitivity of an actor to low-level or ambiguous space incidents. It captures how quickly a reversible action – such as jamming or shadowing – might escalate into a kinetic or political crisis. Actors

Tab. 2: Operational KPIs for evaluating space deterrence performance

KPI name	Definition	Strategic function
SAI	Degree to which assets and behaviour obscure intent (e.g., dual-use systems)	Assesses escalation risk & signalling clarity
RRM	System's ability to maintain or rapidly restore function post-interference	Evaluates deterrence-by-survivability
TDSR	Alignment between technological capabilities and operational doctrine	Detects doctrinal lag or policy overstretch
EER	Probability of escalation in response to a reversible or ambiguous attack	Measures stability margin in grey zones
CBES	Level of transparency, dialogue and norm promotion with other actors	Indicates soft deterrence through diplomacy

CBES, confidence-building engagement score; EER, escalation elasticity ratio; KPIs, key performance indicators; RRM, resilience readiness metric; SAI, strategic ambiguity index; TDSR, tech-doctrine synchronisation rate.

with high EER are more likely to absorb minor infractions without triggering retaliatory responses, thereby enhancing strategic stability. Low EER, in contrast, reflects rigid doctrines or poor attribution mechanisms, increasing the risk of disproportionate reaction.

The CBES reflects the extent to which an actor engages in transparency, dialogue and norm-shaping initiatives in the space domain. High CBES values indicate proactive participation in confidence-building measures, including bilateral space security dialogues, shared SSA frameworks, or public declarations of intent. These actions strengthen deterrence by enhancing trust, reducing misperceptions and contributing to the emergence of shared behavioural expectations, especially in the absence of binding legal instruments.

The integration of these KPIs into strategic planning processes supports a more dynamic, data-informed and future-resilient approach to deterrence assessment. Rather than relying solely on threat-based calculus or symbolic declarations, decision-makers can track posture health in real time, identify gaps or imbalances and recalibrate their deterrence design accordingly.

Moreover, these KPIs allow for comparative posture mapping across actors – as demonstrated in this article's application to the United States, China and NATO/EU – which can inform alliance coordination, doctrinal refinement and escalation prevention strategies.

In this way, Table 2 marks a conceptual and methodological shift toward strategic foresight and operational measurability, offering a scalable toolset for managing deterrence in a domain characterised by rapid change, multi-actor dynamics and deep uncertainty.

3.4 The TDDM in action

The TDDM posits that deterrence in the space domain must be understood as an evolving, multi-layered process – shaped not only by static capabilities or declaratory policies but also by the interaction of technological readiness, doctrinal coherence and systemic resilience under conditions of uncertainty.

At its core, the TDDM views deterrence as a strategic feedback system. It incorporates five interdependent dimensions – resilience, ambiguity, synchronisation, elasticity and confidence-building – that function dynamically over time. These dimensions do not operate in isolation; they intersect and co-evolve as actors respond to new threats, technologies and behaviours in the orbital domain.

For example, an actor may initially rely on ambiguity to deter aggression (high SAI), but in response to increasing counterspace risks, it may transition toward architectural resilience (high RRM) or greater transparency (high CBES). Similarly, as emerging technologies such as AI and quantum communications enter operational use, the TDSR becomes critical in determining whether such innovations strengthen or destabilise deterrence logic.

This model is inherently adaptive, and allows for strategic recalibration based on evolving threats and shifting environmental conditions. Unlike classical deterrence, which assumes a relatively stable balance of power, the TDDM accounts for rapid technological disruption, multipolar actor dynamics and legal-regulatory fragmentation, all of which redefine how deterrence must be measured and enacted in space.

As a framework, the TDDM is designed not only for theoretical modelling but also for policy application, allowing decision-makers to diagnose weaknesses in current posture, identify areas for investment or coordination and assess the long-term implications of deterrence behaviours across different orbital regimes.

4 Applying the TDDM: strategic postures in practice

To move from theory to practice, this section applies the TDDM to assess and compare the deterrence architectures of three influential actors in the space domain: the United States, China and NATO/European partners. Each actor exhibits distinct approaches to counterspace strategy, resilience, doctrinal development and normative engagement – offering valuable insight into the real-world utility of the proposed framework.

4.1 The United States: deterrence through resilience and redundancy

The United States' contemporary space posture reflects a shift from retaliatory doctrines toward resilience-centric deterrence, as exemplified by the operationalisation of PWSA under the U.S. Space Development Agency. This constellation of hundreds of LEO-based satellites is designed to ensure persistent sensing, secure communication and survivability in degraded or contested space environments.

In parallel, the U.S. has invested heavily in non-kinetic counterspace capabilities, such as cyber tools, directed energy weapons and jammers, as highlighted in the Space Threat Assessment (Swope et al. 2024).

These tools increase its ability to retaliate in reversible and proportionate ways, thereby enhancing deterrence elasticity.

However, the integration of commercial actors into national deterrence strategy introduces a complex duality-generating both enhanced capability and strategic vulnerability. Systems such as Starlink, while enabling agility, redundancy and proliferated architectures, simultaneously introduce escalatory ambiguity, particularly in scenarios involving attacks on dual-use assets. From the perspective of the TDDM, the United States exhibits a medium-to-high SAI, reflecting the blurred distinction between civilian and military space functions. Its RRM is notably high, owing to investments in disaggregated constellations and hardened infrastructure. The TDSR is also high, as the integration of advanced technologies – such as AI-enabled SSA and manoeuvrable satellite platforms – has been consistently aligned with doctrinal evolution. Nevertheless, the EER remains moderate, suggesting that while the U.S. retains flexibility in escalation management, the involvement of commercial actors may constrain decision-making under crisis conditions. Similarly, the CBES is assessed as moderate, given that transparency efforts are often calibrated through strategic communication rather than formal arms control mechanisms or multilateral confidence-building regimes.

4.2 China: precision signalling and strategic ambiguity

China has adopted a strategy of technological opacity combined with targeted signalling, maintaining ambiguity around its co-orbital, rendezvous-capable satellites (e.g., Shijian-21) and ground-based ASAT missile tests, while simultaneously advancing quantum communication satellites (e.g., Micius) and space-based situational awareness.

Beijing's deterrence posture is characterised by a deliberate fusion of denial-centric capability development and sustained doctrinal ambiguity. While Chinese policy statements emphasise the peaceful use of outer space and advocate for non-weaponisation, its strategic behaviour reflects a parallel trajectory focused on counterspace preparedness. In times of crisis, this posture aims to undermine the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) architectures of potential adversaries, thereby neutralising their decision-making advantage. According to the Secure World Foundation's (2024) Global Counterspace Capabilities Report, China has developed a diverse and increasingly sophisticated suite of counterspace tools. These include high-power microwave systems capable of disrupting onboard electronics; co-orbital manoeuvring satellites designed for close-proximity operations; space-based laser dazzlers intended to temporarily blind or degrade optical sensors; and AI-enhanced tracking systems for improved targeting, monitoring and predictive modelling of both debris and active spacecraft. Together, these capabilities enhance China's capacity for strategic denial while reinforcing a deterrence logic that is difficult to decipher and therefore inherently destabilising under ambiguous operational conditions.

This duality-diplomatic signalling on the international stage, juxtaposed with domestic preparedness for disruption-manifests as a form of layered ambiguity that fundamentally complicates the logic of deterrence by punishment. From the vantage point of the TDDM, China exhibits a very high SAI, stemming from its civil–military integration, limited doctrinal transparency and the strategic use of dual-use systems to obscure intent. The RRM is assessed as medium; while China has made measurable progress in redundancy planning and counterspace capability development, it still lacks publicly demonstrated, rapid-recovery architectures on par with those of its competitors. The TDSR is moderate, reflecting a gap between operational advancements – such as co-orbital proximity operations and kinetic ASAT capabilities – and the pace at which these are integrated into open doctrinal discourse. The EER is low, indicating a narrow tolerance for ambiguous or low-level space incidents and a strategic culture that leans toward preemption and coercive signalling. Finally, the CBES is also low, as China has largely refrained from substantive engagement in multilateral risk-reduction dialogues or the establishment of robust transparency mechanisms, thereby limiting its contribution to norm-building in the space domain.

4.3 NATO and European partners: norm-first deterrence and capacity gaps

Europe's approach to space deterrence – particularly through NATO and ESA (European Space Agency) coordination – emphasises strategic stability through normative frameworks, multilateralism and institutional restraint. Rather than projecting deterrence through ambiguity or coercive capability, European actors position themselves as norm entrepreneurs, prioritising rule-based order and collective security over unilateral escalation. The EU Space Strategy for Security and Defence (Clapp and Evroux 2023) explicitly frames the prevention of space militarisation

and armed conflict as a central strategic objective. This posture is operationalised through a set of key priorities, beginning with sustained investment in SSA and space traffic management (STM) capabilities-intended to improve transparency, reduce collision risks and enable early threat detection. In parallel, Europe has launched initiatives to expand its orbital resilience infrastructure, exemplified by projects such as IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite), the sovereign multi-orbit satellite constellation designed to secure communications and critical services. Finally, the EU promotes the codification of responsible behaviours, including voluntary transparency measures, open engagement in norm-setting dialogues, and advocacy for arms control mechanisms tailored to the unique characteristics of the space domain. Together, these priorities form a deterrence posture centred not on denial or ambiguity, but on predictability, institutional legitimacy and the proactive shaping of international space governance.

However, NATO's counterspace capabilities remain largely dependent on U.S. assets, and Europe lacks significant offensive deterrence capacity, limiting its ability to deter through denial or punishment. Growing space congestion and sustainability challenges are of particular concern to European actors (European Space Agency 2025), reinforcing their emphasis on deterrence-by-norms and environmental stewardship. From the perspective of the TDDM, NATO and European partners collectively reflect a deterrence posture rooted in normative engagement and multilateral transparency, rather than coercive capability or strategic opacity. Their SAI is low, indicating a deliberate preference for separating civilian and military functions in space and for maintaining operational openness – an approach that promotes predictability but may limit deterrence-by-uncertainty. The RRM is moderate, owing to growing investments in satellite redundancy and shared situational awareness infrastructures, yet still constrained by dependence on allied systems – particularly those of the United States – for real-time resilience execution. The TDSR ranges from low to moderate, as doctrine tends to lag behind technological adoption across disparate member states, and cohesive alliance-wide strategic integration remains incomplete. In contrast, NATO/EU actors score high on the EER, reflecting a pronounced institutional inclination toward strategic restraint, de-escalation and multilateral consultation, particularly in response to ambiguous or low-intensity provocations. Their CBES is likewise high, as European space actors have consistently championed transparency initiatives, international legal frameworks and the development of soft deterrence norms through civil–military partnerships and cross-domain dialogue. Together, these indicators position NATO and the EU as normative stabilisers in the space domain, albeit with operational limitations in autonomous deterrence execution.

4.4 Mapping deterrence postures: comparative analysis of strategic actors

The complexity of space deterrence is not only technological but also strategic and cultural. Different actors interpret, construct and deploy deterrence logic in alignment with their unique national doctrines, governance architectures and operational capacities. To demonstrate the diagnostic utility of the TDDM, this section applies its core KPIs across three key strategic actors: the United States, China and NATO/European partners.

This comparative assessment highlights not only variations in posture but also divergent philosophies of deterrence, offering a cross-sectional view of how resilience, ambiguity, synchronisation, elasticity and normative engagement are distributed across the global deterrence landscape.

Table 3 operationalises the TDDM framework by mapping each actor's deterrence posture across five performance dimensions. This comparative matrix illustrates how different strategic cultures and institutional logics prioritise specific components of deterrence, resulting in varying levels of strategic stability, escalation management and signalling effectiveness.

The SAI reflects the degree to which dual-use technologies and behavioural opacity are leveraged. The RRM captures architectural survivability and operational continuity. The TDSR assesses doctrinal responsiveness to emerging capabilities. The EER estimates tolerance for ambiguous incidents. Finally CBES captures soft deterrence through transparency and norm promotion.

The result is a multidimensional deterrence profile for each actor, revealing both strengths and vulnerabilities in posture configuration. Importantly, these differences reflect deeper structural choices: whether to pursue deterrence through capability denial, coercive uncertainty, or normative alignment.

4.4.1 United States: resilience-first deterrence

The United States exhibits a moderate-to-high SAI, driven by the integration of dual-use commercial assets

Tab. 3: Comparative strategic postures through the TDDM lens

Actor	SAI	RRM	TDSR	EER	CBES	Normative posture
United States	Med–high	High	High	Moderate	Moderate	Strategic resilience + response
China	Very high	Medium	Moderate	Low	Low	Strategic ambiguity + denial
NATO/EU	Low	Medium	Low–mod	High	High	Normative anchoring + diplomacy

CBES, confidence-building engagement score; EER, escalation elasticity ratio; RRM, resilience readiness metric; SAI, strategic ambiguity index; TDDM, technologically dynamic deterrence model; TDSR, tech-doctrine synchronisation rate.

like Starlink and the deployment of manoeuvrable military satellites. While this ambiguity serves as a deterrent by complicating adversary targeting decisions, it also raises the risk of misperception. The U.S. also demonstrates a deterrence posture anchored in strategic resilience and active response capability. With significant investments in disaggregated architectures (e.g., PWSA), hardened satellite systems and cyber-physical redundancies, the U.S. maintains a high RRM score, reflecting its emphasis on deterrence-by-denial and survivability under attack. The TDSR is high, indicating an institutional capacity to integrate emerging technologies-AI, SSA systems, quantum communications – into strategic doctrine. However, the EER remains moderate, as U.S. deterrence logic includes thresholds for retaliatory escalation, particularly in response to attacks on commercial or critical infrastructure. Its engagement in confidence-building is moderate and often filtered through broader strategic communication platforms (e.g., DoD space strategies, declaratory policies). Collectively, the U.S. embodies a resilience-first doctrine that merges technological superiority with flexible, calibrated response planning.

4.4.2 China: precision disruption and opacity

China's deterrence posture is characterised by a deliberate use of strategic opacity and calibrated ambiguity. Its space programme integrates civil–military fusion, which complicates attribution and intent analysis. The result is a very high SAI-China leverages uncertainty as both a shield and a deterrent mechanism. China's RRM is moderate, with growing investments in redundancy and SSA infrastructure but limited demonstrated capacity for real-time recovery. Notably, its TDSR is moderate, as doctrinal publications remain sparse and largely reactive. While technologically capable – especially in satellite rendezvous, kinetic ASAT and quantum communication – China's public doctrine often lags behind operational advances, limiting strategic transparency. Its EER is low, reflecting a relatively rigid posture toward perceived threats and a doctrinal emphasis on preemption and anti-access/area denial (A2/AD) capabilities. Its confidence-building engagement is minimal, limited to intermittent participation in multilateral dialogues and the occasional issuance of high-level declaratory statements. Overall, China's deterrence model reflects an emphasis on coercive uncertainty, leveraging ambiguity and reversibility while maintaining doctrinal opacity and escalation asymmetry.

4.4.3 NATO/EU: normative posture with capacity gaps

With a low SAI, NATO/EU actors emphasise civilian–military separation and behavioural openness. However, this comes with trade-offs in strategic ambiguity and deterrence-by-uncertainty. NATO and European actors collectively represent a deterrence paradigm grounded in normative anchoring and diplomatic engagement. Although their RRM is moderate, reflecting reliance on allied capabilities (notably U.S. assets), their posture is less about denial and more about stability through transparency. Their TDSR is low to moderate, reflecting doctrinal fragmentation across member states and slower integration of emerging technologies into operational strategy. Crucially, their EER is high, signalling a preference for strategic restraint in response to ambiguous incidents. This posture lowers the risk of inadvertent escalation but may reduce credibility against more assertive adversaries. Their confidence-building engagement is the highest among the three actors, encompassing transparency initiatives, multilateral cooperation, support for international law and civil–military governance. These behaviours reinforce NATO/EU as norm entrepreneurs in the orbital domain. Thus, NATO and EU deterrence is structured less around coercion and more around stability, predictability and institutional legitimacy.

4.4.4 Strategic convergence and fragmentation risks

This comparative application of the TDDM reveals significant divergence in deterrence philosophies and

performance dimensions across major space actors. While this variation reflects differing political systems, threat perceptions and alliance dynamics, it also generates doctrinal misalignment, particularly in response to shared threats such as reversible counterspace attacks, commercial interference, or ambiguous manoeuvres. The absence of common thresholds and interpretive frameworks risks misperception, escalation asymmetry and breakdowns in signalling – especially under crisis conditions. At the same time, each actor's unique deterrence architecture offers opportunities for cross-learning, collaborative threat modelling and minilateral norm-setting in areas of convergence, such as SSA data exchange, dual-use satellite management and AI governance. The TDDM thus serves as both a diagnostic lens and a bridge-building instrument, enabling strategic planners to identify structural gaps, evaluate posture stability and anticipate escalation risks in an increasingly contested orbital environment.

4.5 Strategic implications

The comparative application of the TDDM reveals a fragmented deterrence landscape marked by structural asymmetries, doctrinal divergence and strategic signalling inconsistencies. These differences are not merely artefacts of political ideology or resource disparity – they reflect fundamentally distinct deterrence philosophies shaping how actors assess threats, configure posture and manage escalation in the space domain.

The United States advances a deterrence architecture centred on resilience and flexible response, combining high levels of technical readiness with multi-domain doctrinal integration. Its ability to rapidly adapt to emergent threats through technological layering and mission assurance underscores a survivability-focused deterrent logic. However, its reliance on commercial dual-use infrastructure introduces ambiguity in attribution and escalatory thresholds.

China, in contrast, embraces a model of strategic ambiguity and calibrated opacity, where deterrence is achieved through unpredictability, low observability and anti-access denial strategies. This posture prioritises coercive flexibility while resisting normative constraints and formalised transparency. Although tactically advantageous, such opacity increases the risk of misperception and escalation mismanagement in crisis scenarios.

NATO and European partners articulate a normatively anchored deterrence paradigm, emphasising transparency, rule-of-law commitments and diplomatic signalling over kinetic denial. This posture promotes crisis stability and soft deterrence but suffers from fragmented doctrine and limited autonomous capability, which may constrain its ability to deter high-end coercion or respond rapidly in contested environments.

Taken together, these strategic variations pose significant risks for doctrinal misalignment, particularly in high-friction scenarios where the clarity of intent and attribution is obscured. Situations involving attribution-deficient incidents, such as electromagnetic interference, global positioning system (GPS) spoofing, or cyber intrusions, present substantial challenges to proportional response and escalation control. Similarly, the increasing prevalence of reversible grey-zone counterspace operations, including non-kinetic techniques like dazzling or jamming, blurs the threshold for what constitutes a hostile act, complicating deterrence signalling. Moreover, disruptions targeting civilian or commercial space infrastructure, especially dual-use satellite networks and privately operated constellations, further erode the boundary between national defence imperatives and economic security, amplifying the risk of inadvertent escalation or norm destabilisation.

The absence of a shared deterrence grammar – both conceptually and operationally creates a volatile ecosystem in which intentions are unclear, red lines are ambiguous and escalation dynamics are difficult to predict or manage.

In this context, the TDDM offers more than a diagnostic lens; it provides a conceptual foundation for strategic convergence. By establishing shared performance dimensions – resilience, ambiguity management, doctrinal synchronisation, escalation elasticity and confidence-building offers decision-makers a common evaluative language through which to compare postures, identify risk asymmetries and promote deterrence harmonisation across actor types.

Moreover, the application of TDDM across geopolitical blocs opens space for minilateral collaboration, including joint posture audits, resilience benchmarking and KPI-based transparency protocols. These initiatives can bridge the current doctrinal gaps and mitigate the risk of inadvertent escalation by fostering a functional dialogue on space deterrence design-even in the absence of comprehensive treaty-based governance.

Thus, the strategic implication of this framework is both analytical and normative: deterrence in the space domain must evolve as a pluralistic, adaptive ecosystem capable of absorbing divergence while steering towards a baseline of shared strategic logic.

4.6 Note on Scope: the exclusion of Russia from the primary comparative framework

Although Russia remains a key actor in the evolving military space landscape, this study deliberately excludes it from the core comparative framework, focusing instead on the United States, China and NATO/European partners. This decision was not based on a dismissal of Russia's counterspace capabilities or strategic relevance, but rather on analytical considerations that support conceptual clarity.

First, Russia's deterrence posture in space exhibits significant thematic overlap with China's model of strategic opacity, reversible counterspace operations and non-declaratory doctrine. Including both actors in a tripolar matrix may have introduced analytical redundancy, particularly in the context of KPIs like SAI or TDSR, where both states exhibit high scores with limited doctrinal transparency.

Second, Russia's public articulation of space deterrence remains highly classified, often reactive, and difficult to assess through open-source strategic materials. Unlike the United States' published strategies or NATO's space declarations, Russian doctrine is embedded in legacy deterrence rhetoric, typically situated within broader nuclear and electronic warfare frameworks. This doctrinal opacity restricts the granularity needed for comparative KPI analysis without introducing speculative assumptions.

Third, the ongoing war in Ukraine has substantially affected Russia's space posture, both in terms of resource reallocation and operational risk behaviour. Russia has reportedly increased electronic warfare activity in the orbital domain, yet also exhibited a growing dependence on external actors, particularly China, for launch services and technological support. In this volatile and transitional context, Russia's deterrence model remains in flux, and may be more appropriately analysed in a dedicated case study or future research effort.

Nevertheless, future iterations of this framework would benefit from incorporating Russia as a distinct deterrence archetype, particularly to explore how post-Soviet strategic thinking adapts (or fails to adapt) to the technological and normative complexities of contemporary spacepower competition.

5 Policy recommendations for adaptive deterrence in the space domain

As the outer space domain evolves into a multipolar, congested and technologically volatile environment, legacy deterrence doctrines-anchored in punitive logic and Cold War dyadic structures-struggle to deliver strategic stability. In response to this shifting paradigm, this section proposes a suite of policy recommendations rooted in the TDDM, designed to support adaptive deterrence strategies that are resilient, precise and normatively grounded.

Structured around three interdependent pillars-strategic adaptation, technological integration and normative innovation – these recommendations seek to enable decision-makers to recalibrate space deterrence frameworks for contemporary and emerging security realities.

5.1 Strategic adaptation: redefining doctrines for a technologically contested environment

5.1.1 Institutionalise resilience as a deterrent logic

States should integrate resilience not merely as a redundancy measure but as a core deterrent mechanism, capable of dissuading attacks by ensuring strategic futility. Investments in disaggregated satellite constellations, autonomous repositioning capabilities and real-time mission continuity will enhance deterrence-by-denial and signal survivability to potential adversaries.

5.1.2 Operationalise cross-domain deterrence coherence

The emerging threat landscape necessitates the synchronisation of space deterrence with cyber, electronic warfare and AI-enabled decision systems. A flexible architecture that links space incidents to multi-domain response options enhances escalation management and complicates adversary calculus without requiring proportional responses in space.

5.1.3 Incorporate the private sector into deterrence planning

With commercial actors occupying a central role in space infrastructure, states must move beyond *ad hoc* partnerships. Developing shared risk frameworks, dual-use escalation protocols and industry-inclusive attribution mechanisms will reduce vulnerability and ambiguity while reinforcing deterrence credibility across public–private ecosystems.

5.2 Technological integration: embedding deterrence into system architecture

5.2.1 Design deterrence-by-function into future constellations

Spacecraft should be developed with native deterrence features – such as automated manoeuvring, hardening against directed energy threats, cyber-intrusion resistance and rapid reconfiguration. These features contribute to deterrence not through offense, but through projected survivability and operational continuity.

5.2.2 Employ AI for strategic signalling and escalation forecasting

AI can support anomaly detection, predictive behaviour modelling and crisis escalation forecasting. When embedded into SSA systems and command-and-control architectures, AI enhances the speed and precision of deterrent signalling – but must be regulated by transparent doctrinal parameters and human oversight to prevent unintended escalation.

5.2.3 Develop deterrence dashboards based on KPI monitoring

States should institutionalise real-time posture tracking tools, using KPIs such as the SAI and RRM. Such dashboards would allow defence planners to dynamically assess deterrence health, identify threshold vulnerabilities and optimise response posture across conflict spectrums.

5.3 Normative innovation: building trust and stability in a fragmented regime landscape

5.3.1 Promote transparency as a strategic asset

Rather than viewing transparency as a liability, states should leverage it as a controlled signalling instrument. Confidence-building mechanisms – such as behavioural disclosure of satellite missions, transparency in counterspace doctrine and publication of operating principles – can strengthen predictability and stability without compromising operational security.

5.3.2 Establish a multilateral code for reversible counterspace measures

The increasing use of non-destructive, reversible counterspace capabilities (e.g., jamming, dazzling, spoofing) calls for a code of conduct that defines acceptable thresholds, scope and time-bound usage. Modelled after chemical agent restrictions, this norm could clarify strategic boundaries while preserving tactical flexibility.

5.3.3 Create an independent registry of counterspace incidents

To reduce misperception and misattribution, a neutral, international registry – possibly under the auspices of the United Nations Office for Outer Space Affairs (UNOOSA) or a newly established Space Stability Secretariat – should catalogue events such as close approaches, interference attempts and cyber intrusions. Such a repository would enhance strategic pattern recognition, promote accountability and support evidence-based diplomacy.

5.4 Leveraging minilateral platforms for strategic governance

In the absence of a comprehensive global treaty regime capable of regulating the increasingly complex landscape of space security, minilateral platforms – such as the G7, G20 and regional constellations like the Quad or AUKUS – emerge as pragmatic arenas for advancing deterrence-oriented governance. While these platforms lack the universal legitimacy of United Nations-based mechanisms, they offer speed, flexibility and political cohesion that are often absent in broader multilateral negotiations.

These groups are uniquely positioned to act as deterrence anchors-coalitions of technologically advanced and strategically aligned states that can pilot new norms, coordinate defensive architectures and promote mutual understanding among spacefaring powers. Their relative institutional agility allows them to respond quickly to the normative and technological disruptions that characterise the contemporary orbital environment.

One core opportunity lies in the establishment of space strategic stability dialogues (SSSDs) under the auspices of such platforms. These dialogues could serve as semi-formal but structured venues for discussing red

lines, escalation management protocols and best practices in dual-use satellite transparency. Unlike formal treaty negotiations, SSSDs could accommodate divergence and uncertainty while still building shared vocabulary and doctrinal literacy among peers.

A second mechanism involves the development of minimum transparency protocols (MTPs) – a practical, non-binding framework encouraging members to disclose limited operational data such as satellite purpose, orbital behaviour anomalies, or the existence of proximity operations. These protocols would not constrain sovereign freedom of action but would serve to reduce ambiguity-driven escalation and demonstrate responsible stewardship.

Furthermore, minilateral platforms can play a catalytic role in shaping public–private threat-sharing frameworks, particularly given the increasing entanglement of commercial actors in critical space infrastructure. By encouraging standardised reporting mechanisms, incident attribution collaboration and resilience co-investment models, these coalitions can foster greater coherence across national security and commercial deterrence postures.

In essence, minilateral groupings provide a strategic middle ground-more dynamic than global regimes, yet more inclusive and transparent than bilateral security arrangements. They serve as bridging institutions, capable of harmonising fragmented deterrence doctrines while offering an incubator for scalable policy innovation in a rapidly evolving space order.

5.5 Policy levers and their strategic function

Table 4 consolidates the care policy levers proposed in this section and situates them within the broader logic of adaptive deterrence. Each lever represents a practical pathway for states to enhance their space deterrence posture, aligned with the principles of the TDDM. The corresponding deterrent effects and strategic functions are not discrete, but interlinked and mutually reinforcing, enabling a layered deterrence ecosystem that is dynamic, resilient and strategically coherent.

Each policy lever is elaborated below to demonstrate how it contributes to deterrence not through traditional force projection, but by altering the cost–benefit calculus, increasing system survivability and managing strategic perceptions in a contested orbital environment.

'Disaggregated Satellite Architectures' reflect a shift from monolithic, high-value assets to distributed constellations that enhance redundancy, complicate targeting and ensure continuity of operations under threat. By rendering adversary attacks operationally futile, this architecture enacts a form of deterrence-by-futility, disincentivising aggression due to the low probability of decisive gains.

'AI-Enabled Escalation Prediction' tools enable states to detect early indicators of grey-zone activity, model adversary behaviour and forecast escalation pathways with increased precision. This supports deterrence-by-foresight, allowing for timely and proportionate signalling while reducing the likelihood of inadvertent or premature escalation. When paired with human oversight and doctrinal integration, AI becomes a force multiplier for strategic stability.

'KPI-Based Posture Monitoring', as outlined in the TDDM, introduces a quantitative layer to strategic decision-making. By tracking metrics such as the SAI or RRM, states can engage in deterrence-by-adaptation – dynamically recalibrating posture based on evolving threat environments and internal performance thresholds.

'Confidence-Building Mechanisms' serve to reduce misinterpretation and lower the risks associated with attribution uncertainty. Initiatives such as behavioural transparency, cooperative SSA, or declaratory policies support deterrence-by-trust, where the probability of crisis miscalculation is minimised through clear and credible signalling of intent.

Tab. 4: Policy levers for adaptive space deterrence and their strategic functions

Policy lever	Primary deterrent effect	Strategic function
Disaggregated satellite architectures	Deterrence-by-futility	Enhances resilience and redundancy
AI-enabled escalation prediction	Deterrence-by-foresight	Supports rapid, calibrated response
KPI-based posture monitoring	Deterrence-by-adaptation	Enables real-time risk assessment
Confidence-building mechanisms	Deterrence-by-trust	Reduces ambiguity and misperception
Reversible weapon norms	Deterrence-by-restraint	Clarifies acceptable operational boundaries
Public–private integration protocols	Deterrence-by-cohesion	Closes attribution gaps and aligns priorities

KPI, key performance indicator.

'Reversible Weapon Norms' introduce behavioural boundaries around tools such as jamming, dazzling, or cyber interference – capabilities often favoured for their non-kinetic and deniable characteristics. Establishing norms of restraint around such actions contributes to deterrence-by-restraint, preserving escalation elasticity while preventing strategic ambiguity from undermining stability.

'Public–Private Integration Protocols' acknowledge the increasing entanglement of commercial actors in national space security ecosystems. By institutionalising communication channels, joint attribution procedures, and shared risk doctrines, states can enact deterrence-by-cohesion. This ensures that public and private interests are strategically aligned, thereby reducing exploitable gaps in deterrence architecture that is not only technically resilient but also strategically modular and normatively grounded.

Taken together, these policy levers offer a holistic toolkit for constructing a deterrence posture that is not only technically resilient and strategically agile, but also normatively grounded and diplomatically credible. Their layered deployment reinforces the core logic of TDDM: that space deterrence in the 21st century must be dynamic, multidimensional and co-evolved with the technologies and actors that shape the domain.

6 Conclusion and future research agenda

Outer space has decisively transitioned from a domain of scientific inquiry and symbolic exploration to a contested arena of strategic interaction, technological disruption and geopolitical entanglement. As the orbital environment becomes increasingly saturated with both state and non-state actors, and as EDTs continue to outpace governance frameworks, the imperative to reconceptualise deterrence is no longer academic – it is strategic.

This article has argued that classical deterrence theories, rooted in the nuclear logic of MAD and predicated on assumptions of dyadic symmetry, transparent signalling and slow decision cycles, are no longer sufficient for managing the risks and complexities of contemporary space-power competition. The rise of non-kinetic, reversible counterspace capabilities; the proliferation of dual-use systems; and the emergence of autonomous, machine-speed architectures have all contributed to the erosion of the strategic clarity upon which traditional deterrence logic depends.

In response, this study has introduced the TDDM – a multidimensional, layered and adaptive framework for evaluating and enhancing deterrence in the space domain. Grounded in five interdependent pillars – resilience, ambiguity management, cyber-physical integration, normative engagement and KPI-based monitoring – the TDDM provides both a theoretical and operational toolkit for navigating the deterrence challenges of a technologically accelerated and strategically fragmented orbital environment.

The comparative application of this model to the United States, China and NATO/European actors demonstrated its diagnostic utility and revealed three distinct deterrence paradigms: resilience-first, ambiguity-centric and norm-driven postures. This diversity, while reflective of divergent strategic cultures and capabilities, also signals the potential for misalignment, misperception and norm erosion – particularly in crisis scenarios involving dual-use ambiguity or attribution uncertainty. The TDDM offers a means to bridge these conceptual and doctrinal divides, enabling more coherent cross-actor assessment and future-proof deterrence design.

The policy recommendations outlined in this article – from embedding deterrence into system architecture and leveraging AI for strategic forecasting, to developing minilateral confidence-building mechanisms – emphasise the need for deterrence to evolve in tandem with the systems, actors and escalation pathways it seeks to influence. Deterrence, in the age of orbital complexity, must become an ecology of strategic design, not a singular doctrine of punishment or denial.

6.1 Future research directions

While this article provides a foundational model and comparative framework, it also reveals critical knowledge gaps and invites deeper scholarly exploration across multiple dimensions. Key avenues for future research include:

6.1.1 KPI operationalisation and simulation modelling

Future studies should formalise the TDDM's proposed KPIs through simulation environments, strategic gaming and escalation modelling. These tools can stress-test how variables such as ambiguity, resilience and elasticity impact deterrence stability under varying crisis scenarios.

6.1.2 AI and automated deterrence dynamics

As AI increasingly mediates orbital decision-making, further research is needed into how machine agents interpret – or potentially misinterpret – strategic intent. What constitutes credible signalling in a human–AI–hybrid deterrence ecosystem?

6.1.3 Non-state actor deterrence and governance

With commercial entities now integral to orbital infrastructure, the boundaries of deterrence must expand to include the co-optation or deterrence of private sector actors. Future work should examine how public–private threat architectures are negotiated, aligned and regulated across diverse jurisdictions.

6.1.4 Deterrence equity and the global south

Current deterrence frameworks largely reflect the perspectives of dominant spacefaring powers. There is an urgent need to assess how emerging actors – particularly those from the Global South – interpret deterrence postures and participate in shaping norms, rights and risk mitigation mechanisms in space.

6.1.5 Orbit-specific deterrence architectures

As strategic activity expands into MEO, GEO and cislunar space, researchers must interrogate whether deterrence principles are altitude-dependent. Do latency, surveillance limitations and spatial-temporal asymmetries alter the efficacy of deterrent signalling across orbital regimes?

In sum, the TDDM is not simply a conceptual contribution – it is a strategic imperative. In an orbital environment defined by rapid technological disruption, geopolitical diffusion and normative ambiguity, deterrence must be understood as a living, adaptive system rather than a static doctrine. Scholars, defence planners and policymakers must now move beyond legacy paradigms rooted in Cold War logic and begin to construct deterrence architectures that are responsive, pluralistic and performance-driven. The TDDM offers not only a framework for diagnosing vulnerabilities and modelling posture health, but also a roadmap for fostering strategic coherence in a multipolar space order. Future stability in space will not be a product of technological dominance alone, but of conceptual agility, institutional coordination and sustained commitment to adaptive deterrence design.

Declaration of interests

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Competing interests

The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy, view or position of any agency, organisation, employer, or company the author represents.

Ethical statement

This paper meets the research and publication ethics standards.

Funding

Not applicable.

References

Al-Rodhan, N. (2023). *Preventing the Increased/Uncontrolled Militarisation of Outer Space*. The Geneva Centre for Security Policy, Geneva.

Berglund, A. (2024). *The Space Development Agency and the Future of Defense Space Acquisitions*. The Center for Space Policy and Strategy, El Segundo, CA.

Bertolini, M., Minicozzi, R., & Sweijs, T. (2023). *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies, The Hague.

Carey, M., & McGillis, C. (2024). Navigating the gray zone: Reframing space strategy for contemporary operational environments. *Journal of Indo-Pacific Affairs*, *7*(4), pp. 97-113.

Cavaciuti, A., Heying, J., & Davis, J. (2022). *In-Space Servicing, Assembly, and Manufacturing for the New Space Economy*. Center for Space Policy and Strategy, El Segundo, CA.

Clapp, S., & Evroux, C. (2023). *EU Space Strategy for Security and Defence*. European Parliamentary Research Service, Brussels. doi: 10.1007/s11695-022-06445-7

Coletta, D. (2023). Deterrence. In: Mayer, S. (ed.), *Research Handbook on NATO*. Edward Elgar Publishing, Cheltenham, pp. 222-236.

Dugger, A. T. (2025). *Space as a Gray Zone: The Future of Orbital Warfare*. Modern War Institute. Available at https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/ [accessed 14 February, 2025]

Elefteriu, G. (2024). *The Role of Space Power in Geopolitical Competition*. Council on Geostrategy, London.

European Space Agency. (2025). *ESA'S Annual Space Environment Report*. ESA, Germany.

Farrell, K. (2024). Controlling the Final Frontier: Balance of Power as a Determinant of Military Strategy in Space. MA thesis, University of Chicago, Social Sciences Division, Chicago.

Filippidou, A. (2020). Deterrence: Concepts and approaches for current and emerging threats. In: Filippidou, A. (ed.), *Deterrence*. Springer, Cham, pp. 1-18. doi: 10.1007/978-3-030-29367-3_1

Flanagan, S. J., Martin, N., Blanc, A. A., & Beauchamp-Mustafaga, N. (2023). *A Framework of Deterrence in Space Operations*. RAND Corporation, Santa Monica, CA.

Garretson, P. (2021). What war in space might look like circa 2030–2040. In: Sokolski, H. D. (ed.), *Space and Missile Wars: What Awaits*. The Nonproliferation Policy Education Center, Arlington, VA, pp. 6-60.

Gartzke, E., & Lindsay, J. R. (2024). Elements of Deterrence: Strategy, Technology, and Complexity in Global Politics. Oxford University Press, Oxford.

Ghoshal, D. (ed.). (2023). Historical and contemporary missile development: Nuclear weapon states, regional powers and other powers. *Role of Ballistic and Cruise Missiles in International Security*. Springer, Cham, pp. 69-143. doi: 10.1007/978-3-031-48063-8_5

Gurantz, R. (2024). *Satellites in the Russia-Ukraine War*. USAWC Press, Carlisle Barracks, PA.

Harrison, T., Johnson, K., & Young, M. (2021). *Defense against the Dark Arts in Space*. Center for Strategic & International Studies, Washington, DC.

Hersman, R. K. C., Williams, H., & Claeys, S. (2022). *Integrated Arms Control in an Era of Strategic Competition*. Rowman & Littlefield Publishers, Lanham, MD.

Jervis, R. (1976). *Perception and Misperception in International Politics*. Harvard University Press, Cambridge, MA.

Jervis, R. (2002). Mutual assured destruction. *Foreign Policy, 133*, pp. 40-42. doi: 10.2307/3183553

Kahan, D. M. (1999). The secret ambition of deterrence. *Harvard Law Review, 113*(2), pp. 413-500. doi: 10.2307/1342330

Lambakis, S. (2022). Space as a warfighting domain: Reshaping policy to execute 21st century spacepower. *Comparative Strategy, 41*(4), pp. 331-369. doi: 10.1080/01495933.2022.2087419

Long, A., & Green, B. R. (2015). Stalking the secure second strike: Intelligence, counterforce, and nuclear strategy. *Journal of Strategic Studies, 38*(1–2), pp. 38-73. doi: 10.1080/01402390.2014.958150

Lucarelli, S., Marrone, A., & Moro, F. (2021). *NATO Decision-Making In the age of Big Data and Artificial Intelligence*. NATO Allied Command Transformation (ACT). https://www.iai.it/sites/default/files/978195445000.pdf

Mazarr, M. J. (2018). *Understanding Deterrence*. RAND Corporation, Santa Monica, CA.

Miller, G. D. (2021). Preventing war with a warfighting domain: Nuclear deterrence lessons for space. *Astropolitics, 19*(1–2), pp. 33-61. doi: 10.1080/14777622.2021.1994338

NATO Science & Technology Organization. (2023). Science & technology trends 2023–2043. *Volume 1: Overview*. NATO Science & Technology Organization, Brussels.

New Space Economy. (2025). Understanding Space Policy: A Guide for Everyone. New Space Economy. Available at https://newspaceeconomy.ca/2025/07/14/understanding-space-policy-a-guide-for-everyone/ [accessed 9 August, 2025].

Oche, P. A., Ewa, G. A., & Ibekwe, N. (2021). Applications and challenges of artificial intelligence in space missions. *IEEE Access, 12*, pp. 44481-44509. doi: 10.1109/access.2021.3132500

Pape, Jr., R. A. (1992). Coercion and military strategy: Why denial works and punishment doesn't. *Journal of Strategic Studies, 15*(4), pp. 423-475. doi: 10.1080/01402399208437495

Peace, N. A. (2023). Space denial: A deterrence strategy. *Joint Force Quarterly, 111*, pp. 58-66.

Pražák, J. (2021). Dual-use conundrum: Towards the weaponization of outer space? *Acta Astronautica, 187*, pp. 397-405. doi: 10.1016/j.actaastro.2020.12.051

Rice, D. M. (2023). Deterrence and Space Strategy: A Framework from the Study of History and Theory. Air University Press, Maxwell Air Force Base, Alabama.

Samson, V. (2024). Space and Counterspace Technologies: Assessing the Current Threat Environment. Observer Research Foundation, New Delhi.

Schelling, T. C. (1962). The role of deterrence in total disarmament. *Foreign Affairs, 40*(3), p. 392. doi: 10.2307/20029563

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

Secure World Foundation. (2024). In: Weeden, B., & Samson, V. (eds.), *Global Counterspace Capabilities*. Secure World Foundation, Washington, DC.

Slingshot Aerospace. (2024). *State of Satellite Deployments & Orbital Operations*. Available at https://www.slingshot.space/news/state-of-satellite-deployments-and-orbital-operations-2023

Svoboda, M. (2022). The Application of Offensive Realism in Outer Space as a Fifth Operational Domain. Master's thesis, Univerzita Karlova, Prague.

Swope, C., Bingen, K., Young, M., Chang, M., Songer, S., & Foreword, J. (2024). *Space Threat Assessment 2024*. The Center for Strategic and International Studies, Washington, DC.

Tunsjø, Ø. (2022). Combining polarity and geopolitics: The explanatory power of geostructural realism. In: Graeger, N., Heurlin, B., Waever, O., & Wivel, A. (eds.), *Polarity in International Relations: Past, Present, Future*. Springer Nature, Cham, pp. 81-99. doi: 10.1007/978-3-031-05505-8_5

Vlasic, I. A. (1991). The legal aspects of peaceful and non-peaceful uses of outer space. In: Jasani, B. (ed.), *Peaceful and Non-Peaceful Uses of Space*. Routledge, London, pp. 37-55. doi: 10.4324/9781003111016-3

Waltz, K. N. (1979). *Theory of International Politics*. Addison-Wesley Publishing Company, Reading, MA.

Wang, C., Fan, Q., Li, C., & Xu, Y. (2024). China's space science satellite series—A review and future perspective. *Bulletin of the Chinese Academy of Sciences, 38*, p. 2024003. doi: 10.1051/bcas/2024003

Yee, L., Chui, M., Roberts, R., & Issler, M. (2024). *Technology Trends Outlook 2024*. McKinsey & Company, London.