Journal of Aerospace & Security Studies
2025 | Volume IV | pp.1-20

Integrating NLP and Scenario Analysis for the Future of Space Security: A Structured Examination of Online Expert Discourse

Dr Dmitry Erokhin

Abstract

This study conducts a scenario-based analysis of space security by integrating diverse perspectives from online media through advanced Natural Language Processing (NLP). Transcripts from 44 YouTube videos on space security are analysed including expert discussions, current news updates, and a diverse range of opinions to identify 14 key factors having an impact on the development of space security including international security environment, technological dependency, anti-satellite weaponry, space debris, governance, transparency, international cooperation, military organisation, commercial roles, cybersecurity, attack forms, commercial resilience, regulatory compliance, and space weather. Based on these factors, three scenarios of the future are developed: a Cooperative and Resilient Space Environment; a Fragmented and Vulnerable Space Domain; and a Chaotic and Hostile Space Environment. The stable future foresees strong international norms, robust cybersecurity, unified military organisation, and high commercial resilience, while the quasi-stable future reflects weakening international relations and governance. The unstable future is shaped by escalating geopolitical tensions, aggressive weaponisation, extreme debris, and severe space weather, leading to widespread disruption. This innovative methodology transforms unstructured online opinions into structured insights to guide policy and strategic decision-making.

Keywords: Space Security, Scenario-Based Analysis, Online Media Analysis, Natural Language Processing (NLP), Policy and Strategic Decision-Making.

Introduction

Space security has emerged as a critical area of study due to the increasing reliance on space-based assets for global communications, navigation, and defence systems.[1] The space domain faces multifaceted threats, including anti-satellite (ASAT) weapons, hypersonic technology, and cybersecurity risks to satellite systems. The rapid deployment of new space technologies introduces additional vulnerabilities to an already complex security environment. Addressing these challenges requires a comprehensive strategy encompassing deterrence, defence, global engagement, situational awareness, and responsive infrastructure.[2]

The increasing importance of space security extends beyond national borders, impacting international stability, economic prosperity, and technological progress.[3] As space becomes a contested domain, the risk of conflict has heightened due to geopolitical tensions and technological advancements. The threat of cyberattacks on space systems is a growing concern, with potential for novel attack scenarios that could catch defenders off guard.[4] Space systems are increasingly linked to societal resilience, necessitating their consideration in future planning.[5] The current volatile, uncertain, complex, and ambiguous (VUCA) environment in space operations presents unique challenges for both government and commercial entities.[6] Strategic foresight emerges as a crucial approach for navigating this uncertainty, enabling better decision-making and increasing resilience to disruption in the space industry. By systematically combining

1 Radosław Bielawski, "Space as a New Category of Threats to National Security," *Safety & Defense* 5, no. 2 (2019): 1–7; Jordan Plotnek and Jill Slay, "New Dawn for Space Security," in *Proceedings of the International Conference on Cyber Warfare and Security*, vol. 17, no. 1 (2022): 253–61 (Reading: Academic Conferences International Limited, 2022).

2 James D. Rendleman, "Strategy for Space Assurance," in *Space Strategy in the 21st Century*, 77–119 (London: Routledge, 2013).

3 Jahid Hasan Rana, Md Rakib, Joy Mondal, and Razon Ali, "Modern Security Dilemma: A Space Security Perspective for the Future World," *International Journal of Research and Innovation in Social Science* 8, no. 3s (2024): 1681–99.

4 Patrick Lin et al., "Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise," *arXiv preprint* arXiv:2406.12041 (2024), https://doi.org/10.48550/arXiv.2406.12041.

5 Liviu Mureşan and Alexandru Georgescu, "The Road to Resilience in 2050: Critical Space Infrastructure and Space Security," *The RUSI Journal* 160, no. 6 (2015): 58–66.

6 Sarah Georgin and Kara Cunzeman, "A Recent Study into the Future of Exploration," in *Proceedings of the AIAA SciTech 2024 Forum*, Orlando, Florida, January 8–12, 2024 (Reston, VA: American Institute of Aeronautics and Astronautics, 2024), paper 2174.

different values of critical factors, scenario planning allows for the anticipation of a range of possible outcomes. This approach not only helps to identify potential risks and vulnerabilities but also informs the development of robust strategies that can adapt to rapidly changing conditions.

Against this background, the aim of this study was to construct plausible scenarios of the future of space security. A scenario includes both the endpoint and the pathway or sequence of events leading to it.[7] To do that, 44 relevant YouTube videos on space security were identified, and their transcripts were extracted. Then, advanced Natural Language Processing (NLP) was applied to identify key factors influencing space security, and finally, three future scenarios were constructed based on a plausible combination of these factors. This approach allows capturing a wide array of perspectives and complements traditional stakeholder workshops or roundtables, which are, while invaluable, inherently limited by the number and diversity of participants.

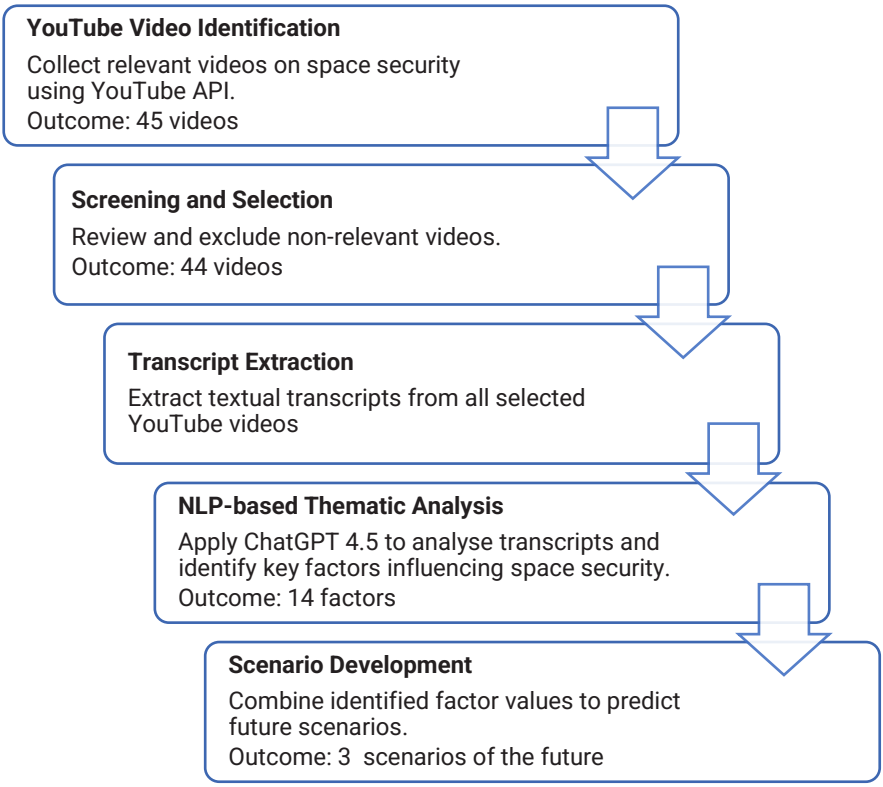
The future scenarios offer valuable insights into how different configurations of the identified factors might influence space security. By presenting these divergent futures, the study underscores the importance of proactive and adaptive policy interventions. The scenarios not only highlight potential risks but also serve as a basis for exploring the range of strategies that could mitigate these threats. This includes developing robust regulatory frameworks, investing in resilient cybersecurity infrastructure, fostering international cooperation, and ensuring that commercial innovations are integrated into a secure and sustainable space environment. The diverse perspectives captured from online media add a layer of depth to the analysis, ensuring that the scenarios reflect a realistic spectrum of opinions and expert insights.

Methodology

In this study, a multi-step methodology was employed to assess the factors impacting space security by leveraging online media sources and advanced NLP (see Figure I):

7 Hannah Kosow and Robert Gaßner, *Methods of Future and Scenario Analysis*, Studies 39 (Bonn: German Development Institute, 2008), https://www.idos-research.de/uploads/media/Studies_39.2008.pdf.

Figure I: Research Methodology Flowchart



Source: Author's own.

First, on 3 March 2025, relevant YouTube videos on space security were identified using the YouTube API, which initially provided 45 most relevant videos to the topic of space security. After closer analysis, 1 video was excluded as non-relevant, resulting in a final set of 44 videos. Most relevant in this context refers to videos that are most likely to appear when someone searches for this topic. All videos, along with short descriptions, are listed in the appendix. This extensive dataset provided a broad spectrum of online opinions, debates, and expert discussions, thereby offering a more comprehensive perspective than traditional stakeholder workshops or roundtables might yield.

Subsequently, the collected transcripts were analysed using ChatGPT 4.5. This advanced language model was utilised to identify key factors influencing space security and to determine the various values associated with each factor. The analysis involved processing the textual data to extract and classify themes related to space security. By automating this thematic extraction, the study

complements direct stakeholder engagement, capturing a richer diversity of opinions and insights from online content.

Based on the identified factor values, a series of plausible scenarios of the future were formulated. These futures are synthesised from different combinations of the values, resulting in detailed narratives that span from stable to unstable outlooks on the future of space security. This scenario-based approach enables the exploration of diverse potential futures and provides a structured framework for understanding the interplay between various factors. Consequently, this study contributes to a growing body of research in the emerging field of web mining applications for scenario building.[8]

Despite its strengths, the methodology has several limitations. The analysis is contingent upon the quality and representativeness of the YouTube video transcripts, which may embody inherent biases of the selected media sources. Furthermore, while ChatGPT 4.5 is a powerful tool for thematic extraction and value determination, it may not capture all the nuances that might emerge from direct stakeholder workshops. Finally, the futures generated are plausible constructs based on current data and assumptions and may not fully account for unforeseen technological or geopolitical shifts in the future.

Results and Discussion

Analysis of the transcripts identified a series of critical factors including the international security environment, technological dependency, anti-satellite (ASAT) weaponry, space debris, governance and international norms, transparency and trust, international cooperation, military organisation, commercial sector role, cybersecurity measures, forms of attack, commercial resilience, regulatory compliance, and space weather that collectively inform our understanding of potential scenarios of the future (see Table I for a comprehensive overview of the relevant factors and their potential values):

8 Victoria Kayser and Erduana Shala, "Scenario Development Using Web Mining for Outlining Technology Futures," *Technological Forecasting and Social Change* 156 (2020): 120086; Kim Young-jun, "A Public-Based Exploratory Approach to Technology Foresight: Text Mining and Scenario Planning" (PhD diss., Seoul National University Graduate School, Seoul, South Korea, 2020); Jieun Kim, Mintak Han, Youngjo Lee, and Yongtae Park, "Futuristic Data-Driven Scenario Building: Incorporating Text Mining and Fuzzy Association Rule Mining into Fuzzy Cognitive Map," *Expert Systems with Applications* 57 (2016): 3.

Table I: Factors Influencing Space Security and their Values

Factors	Factor Values			
Factor 1: International Security Environment	Stable (peaceful cooperation, established norms)		Deteriorating (current state, increased tensions and potential for conflict)	
Factor 2: Technological Development and Dependency	Low technological dependency (minimal satellite use)	Moderate technological dependency	High technological dependency (heavy reliance on space technology for communication, transportation, navigation, etc.)	Accelerated technological innovation (disruptive technologies and commercial initiatives rapidly changing the landscape)
Factor 3: Anti-Satellite (ASAT) Weaponry	Non-existent (no ASAT capabilities)	Limited ASAT capability	Extensive development and testing of ASAT weapons (destructive and non-destructive technologies)	Widespread operationalisation (actively deployed and tested by multiple nations, e.g., US, Russia, China)
Factor 4: Space Debris	Minimal debris environment	Moderate debris environment (occasional collisions and manageable risks)	High debris environment (significant risk of collision, frequent manoeuvres required)	Extreme debris environment (critical threat to space assets and astronauts, resulting from ASAT testing)
Factor 5: Governance and International Norms	Strong international norms and agreements (clear and robust regulations widely accepted)	Weak norms but existing informal understandings	Weak governance (few or inadequate regulations, limited international agreements)	No governance (absence of enforceable norms or legal frameworks, high potential for conflict)
Factor 6: Transparency and Trust	High transparency (clear communication of intentions and capabilities, strong international trust)	Moderate transparency (occasional miscommunications or misunderstandings)	Low transparency (ambiguous intentions, insufficient information sharing, rising tensions)	No transparency (significant misunderstandings, high potential for conflict escalation due to mistrust)
Factor 7: International Cooperation	Strong international cooperation (multilateral space security mechanisms)	Moderate cooperation (limited multilateral initiatives)	Limited international cooperation (mostly bilateral agreements, some diplomatic engagement)	Isolationism (countries acting independently, limited or no international cooperation)

Factor 8: Military Organisation and Governance	Unified military organisation (clear command structure and accountability, e.g., unified Space Force)	Fragmented military organisation (responsibilities distributed across multiple branches)	Adaptive governance (responsive, integrated civil-military-commercial governance)	Rigid governance (slow response, outdated regulations)
Factor 9: Commercial Sector Role	Minimal commercial involvement	Growing commercial involvement (commercial satellites supporting military operations and imagery)	Dominant commercial sector (heavy commercial presence driving innovation and security implications)	Regulatory mismatch (laws/regulations not keeping pace with commercial realities, gaps leading to vulnerabilities)
Factor 10: Cybersecurity Measures	High cybersecurity standards (robust encryption, secure ground stations, multi-GNSS receivers)	Moderate cybersecurity standards (partial implementation of security measures, vulnerabilities exist)	Low cybersecurity standards (insufficient security measures, high vulnerability to cyber-attacks, data breaches common)	
Factor 11: Forms of Attack	Direct kinetic attacks (ASAT missiles clearly detectable, attribution is easy)	Non-kinetic reversible attacks (jamming and cyber-attacks; attribution difficult, reversible, covert)	Mixed methods (combination of overt kinetic attacks and covert cyber operations)	
Factor 12: Commercial Sector Resilience	Strong international regulatory compliance (effective global licensing and enforcement, universal standards)	Moderate resilience (some measures in place but insufficient protection against targeted attacks)	Low resilience (minimal or no protective measures, highly vulnerable)	
Factor 13: International Regulatory Compliance and Enforcement	Strong international regulatory compliance (effective global licensing and enforcement, universal standards)	Moderate compliance (partial adherence, occasional breaches with some accountability)	Weak compliance (frequent breaches, limited enforcement, finger-pointing among parties, ineffective regulation)	
Factor 14: Space Weather (Natural Threats)	Stable space weather (minimal solar storms or natural disruptions)	Moderate space weather (occasional events, manageable impacts)	Severe space weather (frequent disruptive events causing significant confusion with man-made attacks)	

Source: Author's own based on factors and their values extracted from YouTube transcripts on space security.

The international security emerged as a foundational factor, ranging from stable conditions characterised by peaceful cooperation and established norms to a deteriorating environment marked by rising tensions and potential conflict. This factor is intrinsically linked with technological dependency, where an accelerated pace of innovation, while driving rapid advancements, also increases reliance on space-based assets critical to communication, navigation, and transportation. In futures where technological dependency is high, vulnerabilities in cybersecurity become more pronounced if corresponding protections are not simultaneously advanced.

ASAT weaponry represents another pivotal element. The transcripts detail a spectrum from limited capabilities where nations maintain modest and controlled ASAT options to widespread operationalisation, in which multiple nations actively deploy such weapons. The extent of ASAT deployment directly influences the physical security of satellites and contributes to the accumulation of space debris. The creation of space debris itself is a factor with values that range from minimal under effective mitigation measures to extreme, where aggressive testing and kinetic engagements generate hazardous levels of orbital debris that threaten both satellites and human activities in space.

The role of governance and international norms cannot be overstated. Strong international agreements and robust regulatory frameworks have the potential to keep space a peaceful domain. Conversely, weak governance or a complete lack of enforceable norms can foster an environment where unilateral actions and escalatory behaviours prevail. In parallel, transparency and trust are critical for maintaining stability; high levels of openness can deter hostile actions by clarifying intentions, while low or absent transparency may lead to misinterpretations and inadvertent escalations, particularly in the cyber realm.

International cooperation further influences the space security domain. A future scenario with strong multilateral cooperation will enable shared space situational awareness and coordinated responses to both kinetic and cyber threats. In contrast, isolationist policies reduce the capacity for collective defence and may lead to fragmented responses to emerging challenges. Similarly, the structure of military organisation ranging from unified and adaptive frameworks to fragmented or rigid governance plays a decisive role in determining how effectively threats are managed. A unified military organisation, such as a well-integrated Space Force, is better positioned to address both physical and cyber threats compared to a fragmented system where responsibilities are dispersed.

The commercial sector's role in space security has grown markedly, with a dominant commercial presence driving innovation and shaping new business

models. However, when commercial activity outpaces regulatory frameworks – a state described as regulatory mismatch – it can introduce vulnerabilities that may be exploited by cyber adversaries. Cybersecurity measures themselves vary from high standards, incorporating robust encryption and resilient ground systems, to low standards where insufficient protection leaves critical infrastructures exposed to cyber-attacks. The nature of potential attacks is also diverse, ranging from direct kinetic strikes, which are overt and highly escalatory, to non-kinetic reversible attacks like jamming and cyber intrusions that are covert and, in some cases, can be mitigated more readily.

Commercial sector resilience, defined by the ability of companies to implement advanced protections and recover from disruptions, further shapes the overall security posture. High resilience helps buffer the impact of attacks, whereas low resilience can lead to cascading failures across critical services. Additionally, international regulatory compliance and enforcement play a crucial role; strong global standards ensure accountability and adherence to rules, while weak compliance mechanisms can lead to frequent breaches and a breakdown in order. Finally, space weather introduces an element of natural uncertainty. Stable conditions allow for predictable operations, but severe space weather events can not only disrupt satellite functionality but also mimic or exacerbate the effects of deliberate cyber or kinetic attacks.

These factors form the basis for the three plausible scenarios of the future formulated in this study (see Table II for plausible combinations of factor values):

Table II: Plausible Combinations of Factor Values and Resulting Future Scenarios

Factors	Scenario 1: Cooperative and Resilient Space Environment	Scenario 2: Fragmented and Vulnerable Space Domain	Scenario 3: Chaotic and Hostile Space Environment
Factor 1: International Security Environment	Stable	Deteriorating	Deteriorating
Factor 2: Technological Development and Dependency	Accelerated technological innovation	High technological dependency	High technological dependency
Factor 3: Anti-Satellite (ASAT) Weaponry	Limited ASAT capability	Extensive development and testing of ASAT weapons	Widespread operationalisation
Factor 4: Space Debris	Minimal debris environment	Moderate debris environment	Extreme debris environment
Factor 5: Governance and International Norms	Strong international norms and agreements	Weak norms but existing informal understandings	No governance
Factor 6: Transparency and Trust	High transparency	Moderate transparency	No transparency
Factor 7: International Cooperation	Strong international cooperation	Moderate cooperation	Isolationism
Factor 8: Military Organisation and Governance	Unified military organisation	Fragmented military organisation	Rigid governance
Factor 9: Commercial Sector Role	Dominant commercial sector	Growing commercial involvement	Regulatory mismatch
Factor 10: Cybersecurity Measures	High cybersecurity standards	Moderate cybersecurity standards	Low cybersecurity standards
Factor 11: Forms of Attack	Non-kinetic reversible attacks	Mixed methods	Direct kinetic attacks
Factor 12: Commercial Sector Resilience	High resilience	Moderate resilience	Low resilience
Factor 13: International Regulatory Compliance and Enforcement	Strong international regulatory compliance	Moderate compliance	Weak compliance
Factor 14: Space Weather (Natural Threats)	Stable space weather	Moderate space weather	Severe space weather

Source: Author's own using plausible combinations of factor values.

Scenario 1: Cooperative and Resilient Space Environment (Stable)

In this envisioned future, international relations and technological innovation converge to create a secure, stable, and dynamic space environment. Nations operate within a framework of peaceful cooperation, underpinned by strong international norms and widely accepted regulations that ensure space remains a domain of shared prosperity and mutual trust.

Global stability is achieved through the steadfast adherence to established norms, with nations engaging in peaceful collaboration and transparent communication. High levels of openness regarding intentions and capabilities foster trust, enabling multilateral security mechanisms and shared space situational awareness to guide decision-making and collective action.

Accelerated technological advancements driven by disruptive commercial initiatives are seamlessly integrated into secure systems. This rapid innovation, coupled with the dominant role of a vibrant commercial sector, ensures that cutting-edge technologies are not only developed swiftly but also safeguarded against emerging threats. Companies have built robust systems, with advanced encryption and diversified support of global navigation satellite systems, that stand resilient against cyber threats and operational interference.

Defensive capabilities are calibrated with restraint: nations maintain modest, controlled anti-satellite options that avoid aggressive escalation. Simultaneously, effective debris-mitigation measures and responsible testing protocols have preserved a minimal debris environment in orbit, ensuring operational clarity and long-term sustainability of space assets.

The establishment of a unified military organisation exemplified by a well-integrated Space Force ensures clear command structures and accountability. This cohesive military governance complements strong international regulatory compliance and enforcement, whereby global licensing and universal adherence to space rules minimise potential conflicts and maintain order.

Space operations are further bolstered by high cybersecurity standards and resilient ground systems. In the event of conflicts, any offensive actions manifest primarily as non-kinetic, reversible cyber intrusions or jamming operations that are promptly detected and mitigated. Meanwhile, a stable space weather environment with minimal natural disruptions contributes to predictable and secure operational conditions.

This image of the future supports both global and regional strategic stability. Strong international norms, robust cooperation, and transparent communication lower the risk of misunderstandings and deliberate escalations. The existence of unified military governance, high regulatory compliance, and resilient commercial and cybersecurity systems ensure that space remains a predictable, secure environment, reducing incentives for arms races or regional power imbalances. Regional actors are included in multilateral frameworks, further reinforcing collective stability.

Scenario 2: Fragmented and Vulnerable Space Domain (Quasi-stable)

In this future, the global space domain is marked by fragmentation and heightened vulnerability. Nations depend heavily on space for essential services such as communication, navigation, and surveillance, yet rising geopolitical tensions and regional disputes increasingly put these critical assets at risk.

Amid a deteriorating international security environment, regional conflicts and escalating tensions create an atmosphere of uncertainty. Heavy technological dependency on space-based systems means that any disruption whether intentional or accidental can have far-reaching impacts on both civilian and military infrastructures. This environment amplifies the risks associated with the development and testing of anti-satellite weapons.

Multiple nations are actively expanding their ASAT programmes, pushing the boundaries of capability without fully operationalising these systems. As a result, the spectrum of potential conflict now includes both overt kinetic actions and covert cyber or jamming operations, complicating the challenge of attribution and response. The blend of these aggressive measures, against a backdrop of high dependency on space assets, creates a precarious balance, where a single misinterpreted action can spark wider escalation.

While space remains an essential domain, the orbital environment is not free from hazards. Occasional collisions and debris events have led to a moderate debris situation, indicating an upward trend in risks that, while still manageable, hint at potential future instability. This growing debris issue further complicates the safe and reliable operation of satellites and other space infrastructure.

The regulatory landscape in space is characterised by weak norms and patchy governance. Although informal understandings and some regulatory frameworks exist, enforcement is inconsistent, and accountability is sporadic. This fragmentation in international regulatory compliance is compounded by moderate

levels of transparency – frequent miscommunications and occasional information withholding undermine trust among nations and within the commercial sector.

The military organisation governing space assets is fragmented, with responsibilities spread across various services and agencies, making coordinated responses challenging in times of crisis. Similarly, while the commercial sector is expanding its role and influence in space, its integration with national security needs is still evolving. Cybersecurity measures within both domains are only moderately robust, leaving critical systems exposed to vulnerabilities and targeted attacks.

Adding to the complexity are natural factors such as occasional solar storms. These space weather events can cause disruptions that are easily mistaken for deliberate actions, further muddying the waters in an already uncertain environment. The convergence of these natural threats with human-induced challenges raises the stakes even higher, increasing the risk of misinterpretation and inadvertent escalation.

Here, strategic stability is mixed and fragile. Weakening international governance, patchy cooperation, and fragmented military organisations create opportunities for regional disputes to escalate or spill over into global instability. The high dependency on vulnerable space assets increases the risk of both intentional and accidental disruptions, while moderate transparency and enforcement gaps heighten the chances of miscalculation. Regional actors may pursue independent or competitive strategies, complicating global efforts to manage stability.

Scenario 3: Chaotic and Hostile Space Environment (Unstable)

In this grim, unstable future, the space domain has transformed into a theatre of chaos and open hostility. Escalating geopolitical rivalries and relentless brinkmanship have pushed international relations to a breaking point, where nations operate under a constant state of alert and distrust. Critical infrastructures on Earth now rely almost exclusively on space-based services, rendering them alarmingly vulnerable in an environment where no robust alternatives exist.

The widespread operationalisation of ASAT weapons marks a dramatic shift in military doctrine. Multiple nations have not only developed but also deployed these weapons as first-strike options, fundamentally altering the calculus of conflict. In this volatile setting, overt, destructive kinetic attacks have become the norm – visible, escalatory, and potentially catastrophic.

Aggressive testing and kinetic engagements have transformed the orbital environment into a hazardous debris field. This extreme level of space debris endangers all assets in orbit, amplifying the risks for both military and commercial systems. The collapse of international regulatory frameworks has left space as a free-for-all arena, devoid of any agreed-upon rules or effective governance.

Transparency has all but vanished, as intentions and capabilities remain shrouded in secrecy. Isolationism dominates, with nations acting independently and rarely engaging in multilateral cooperation. Rigid, outdated military structures further complicate rapid decision-making, impeding the ability to adapt to emerging threats. This combination of factors has fostered an environment where misinterpretations and unintended escalations are inevitable.

While the commercial sector continues to boom, it does so amid a regulatory mismatch that leaves companies highly exposed to exploitation and cyber-attacks. Low cybersecurity standards and insufficient protective measures mean that even minor disruptions can trigger cascading failures across critical systems. Vulnerability of these commercial entities exacerbates overall instability of the space domain.

Compounding the human-driven chaos are severe space weather events. Frequent, intense solar storms disrupt operations and further blur the lines between natural phenomena and hostile actions. These environmental challenges not only hinder operational stability but also serve as an additional source of confusion and tension.

Strategic stability is severely compromised in this future scenario. Widespread operationalisation of ASAT weapons, lack of governance, isolationism, and low transparency create an environment ripe for crisis and uncontrolled escalation. Both global and regional rivalries are likely to intensify, with nations acting unilaterally, often in ways that undermine predictability and deterrence. Vulnerability of the commercial sector and frequent severe space weather add further volatility, making both intentional and accidental destabilising events more likely.

Conclusion

The evolving security landscape of outer space, as revealed through this study, is not merely a set of disparate trends but an intricate system where technological, geopolitical, commercial, and regulatory dynamics interact. The scenario-based approach used here demonstrates that the trajectory of space security cannot be

reduced to linear progress or decline. Rather, it emerges from the interplay and feedback between diverse actors, innovations, and governance mechanisms.

A central insight from this research is that space security is fundamentally relational and interdependent vulnerabilities in one domain (such as cybersecurity or regulatory compliance) propagate rapidly and can be amplified by weaknesses in others (such as international cooperation or military governance). The three future scenarios (cooperative, fragmented, and chaotic) are not isolated endpoints but represent a spectrum along which the global community may shift, sometimes unpredictably, as a result of both deliberate policy choices and exogenous shocks (including severe space weather).

Importantly, this study foregrounds the critical role of regulatory and policy agility. The pace of commercial innovation and technological disruption in space far outstrips current governance frameworks, creating persistent gaps that adversaries may exploit. Therefore, the capacity of institutions to adapt, harmonise, and enforce norms, while actively engaging with the private sector and broader society, will increasingly define resilience of the space domain.

Rather than viewing these scenarios as fixed predictions, they should be understood as navigational tools by policymakers and stakeholders. Each clarifies how particular configurations of risk, cooperation, and governance may produce radically different outcomes. Ensuring a secure and sustainable future in space will require not only technical solutions and robust military deterrence but also the cultivation of trust, transparency, and shared stewardship across borders and sectors.

Ultimately, the findings affirm that the fate of space security will be shaped less by technological inevitabilities than by the choices made today – choices about cooperation, regulation, innovation, and inclusion of diverse perspectives in decision-making. Only through a genuinely integrated, adaptive, and anticipatory approach can humanity hope to secure the long-term benefits of space for all.

Appendix: YouTube Videos Analysed

Video Id	Video Title	Video Content
o77bcFdSbb4	'What is Space Security?'	Dr Jessica West explains why comprehensive governance is needed to ensure the peaceful use of outer space.
c5q5kGzwJqg	'Space Security: What are the Threats'	Todd Harrison discusses longstanding threats to space security and the importance of public awareness.
j6iE62jovMo	'Israel's Former Space Security Chief Claims Aliens Exist, And Trump Knows | NBC News NOW'	NBC News covers claims by Israel's former space security chief that the US has contacted extraterrestrials.
oyy3kX3-KLI	'PSSI Space Security Guest Lecture: Space and Irregular Warfare'	Dr John Klein gives a lecture on the relationship between space and irregular warfare.
worxslP7Jyw	'Space Security - Spacecast 10'	Dr Brian Weeden reviews global counterspace capabilities that could disrupt or destroy space systems.
cSS8BUBZPtY	'How To Make Space Security Work Understanding the Space Domain and Space Systems'	Panel explores how the technical nature of space shapes governance and legal approaches to security.
3CxuMio1NcU	'NBC News reports – Israel's Former Space Security Chief reveals Aliens exists and Trump knows'	NBC News reports on claims that aliens exist and the US government is aware of it.
i-hzZMRSXA4	'Chatham House 2025 | The Battle for Space: Security, Strategy & Survival'	The 2025 Space Security Conference tackles rising competition, conflict risks, and strategies for peace in space.
tf6JtxV1YHg	'21st Century Security in Space'	Video explains how space technology connects and supports global security across all domains.
0kZa2lrqzvo	'Space Security - in 60 seconds'	EU Special Envoy Marjolijn van Deelen summarises why space security matters to daily lives.
lt7hfyTmyfU	'How Space Force is simulating cyberthreats to protect US satellites | Vargas Reports'	NewsNation shows how Space Force simulates cyberthreats to prepare for future space conflicts.
gaTZjmxbVA8	'Challenges to Security in Space 2022'	DIA's 2022 report highlights growing threats from China and Russia to the security and stability of space.

uPhuGAe4lyY	'Chatham House 2025 | ESA's Dr Kai-Uwe Schrogl on Space Security & Cooperation'	Dr Kai-Uwe Schrogl discusses ESA's key role in maintaining peaceful, secure, and cooperative use of space.
urIOxlz6U3o	'SPACE FORCE: The Secret Orbit - Arms Race in Space | SpaceTime - WELT Documentary'	Documentary examines the rise of the U.S. Space Force and renewed arms race in space.
5rdwnPxuLpM	'Outer Space Security Conference 2022 Opening with Robin Geiss and Keynote with Izumi Nakamitsu'	The 2022 UNIDIR Space Security Conference explores the growing risks and governance challenges in outer space.
OaGBxMDmgbo	'Space Security is Your Problem, Too'	Panel discusses why space security concerns everyone, not just major powers, and the roles all sectors can play.
5aV2QWWQmlA	'2024 ASCEND: Space Security & Protection'	ASCEND 2024 focuses on safeguarding space infrastructure through collaboration and innovation.
Em7nsLzs9UA	'How Can Space Security Be Achieved: Past, Present, Future Efforts And Practical Measures For PAROS'	Panel reviews past and current initiatives for space security and lessons for future disarmament efforts.
v9uqNya5-dA	'Dual-use space assets and their impact on space security Outer Space Security Conference 2021'	Experts discuss how dual-use satellites create both opportunities and new risks for space security.
PzguPC6B6fc	'Regional Resilience–Japan's Space Security | The Space Policy Show Ep. 141'	Discussions with experts from Japan's Institute of Geoeconomics on the country's shifting defence posture, growing space partnerships, and importance of regional alliances for security and resiliency in the Asia-Pacific.
M5Kh7D1VPFs	'Thomas Jennewein at the UNIDIR 2018 Space Security Conference'	Thomas Jennewein discusses quantum encryption and the University of Waterloo's science satellite at the 2018 Space Security Conference.
DbavFRYnDig	'ORF-KC 2019 | Space Security'	Panel discusses rising threats from counter-space technologies, real-world incidents, and how nations and commercial actors respond, highlighting the need for dialogue to ensure a stable and sustainable space environment.
b27sv5pBqUw	'2024 ASCEND: Space Security & Protection'	The 2024 ASCEND conference brings together government, industry, and academia to address growing risks to space systems and develop solutions for secure, sustainable space use.

KPuSUk7wsgU	'International Space Security in 2018	Alexandra Stickings discusses the prospects for international space security in the year ahead.
CTiD0rmY99E	'Space Security'	Carnegie Endowment panel on how outer space opens the door to both competition and cooperation between nations.
WyntUBq5SpE	'7th Prague Space Security Conference (June 16-18, 2024)'	The PSSI Space Security Conference Series gathers senior experts from Europe, the US, and Asia to address pressing space security threats, foster strategic partnerships, and advance global stability in the space domain.
Zi346Oo6iNw	'60 Minutes: Satellite security targeted in space'	David Martin of CBS News discusses the dangers posed by newly developed ASAT weapons to national intelligence and communications.
zmg7GKXhFyw	'OS23 Panel III — Future Multilateral Space Sec. Initiatives | Outer Space Security Conference 2023'	Panel discusses how to build on past efforts and prepare for future multilateral space security initiatives.
-E4LsnPqEWg	'Assessing space security: Threat and response'	Brookings discussion about evolving space security threats and effective responses by the US and international community.
Uk5eeGVuMB8	'Former Israeli space security chief says aliens exist, humanity not ready'	Retired Israeli general and former space security chief Haim Eshed claims that Israel and the US have made secret contact with aliens from a 'Galactic Federation,' including alleged cooperation and an underground base on Mars.
hWypV0ElkNE	'What Threatens Space Security? Space Systems and Threat Vectors'	Panel explores the wide range of space security threats including physical, electronic, and cyberattacks from space or the ground.
umsreNQclw0	'Who Can Achieve Space Security? Diversity and Prevention of an Arms Race in Outer Space (PAROS)'	Panel discusses how regional perspectives, multi-stakeholder participation, and gender inclusion are vital for achieving peaceful and secure use of space and advancing PAROS.
sEp_orE7KHE	'Space security issues'	Ifri conference explores the geopolitical context and European efforts in space security, featuring discussions on space tracking, space debris, the EU-SST consortium, and industry perspectives.

_27pD_yZPm0	'2023 ASCEND: The Nexus of Space Security and Protection'	Lauren Smith of Northrop Grumman shares her vision for secure, safe, and open access to space for all at ASCEND 2023.
2T5-mGMhH0s	'OS23 Panel I — Mapping Space Threats, Risk and Challenges | Outer Space Security Conference 2023'	Panel provides an overview of the value of space assets and examines the various threats, risks, and challenges to space security posed by advancing technologies and hostile actors.
2KC67LjeJfo	'Russian Nuclear Weapons in Space? Here's What We Know- WSJ'	Wall Street Journal examines new intelligence on Russia's possible plans to deploy a nuclear weapon in space, its implications for satellites, and the historical context of nuclear detonations like Starfish Prime.
bLZNQMuFogc	'Cyber and Space Security: The New Battlefield | CGFS'	Creative Global Funding Services explores the rapidly evolving challenges and innovations in cyber and space security, highlighting emerging threats, advanced technologies, and the importance of global collaboration for future defence.
PU-mW941LtU	'Space Security: Space Crisis Dynamics Panel'	Panel discusses how the changing space environment and proliferation of counterspace capabilities have complicated crisis dynamics, deterrence, and decision-making, sharing insights from tabletop exercises that simulate space conflict scenarios.
mjv4pHb4wyk	'U.S. Space Force: Major Changes Ahead in Space Security'	The U.S. Space Force is undergoing major changes including restructuring and calls for increased funding to strengthen space security and build a more resilient space architecture.
98naJzVx8Pk	'The Nexus of Space Security & Protection'	Panel explores growing threats to space systems and highlights cybersecurity, partnerships, and new technologies for protecting vital space assets.
N_5SrZB8t4Y	'Protecting the Final Frontier: Cyber Space Security'	Space is the new frontier but is also exposed to cyber threats, making the security of space assets increasingly important.

8emmRJGrimI	'CYSAT 21: James Pavur Adventures in VSAT hacking: lessons for space security'	James Pavur, a Rhodes Scholar and Oxford PhD student, talks about the intersection of cyber-security and space technology, focusing on satellite communications.
Vppj5242Zw0	'2023 ASCEND: The Nexus of Space Security & Protection (Part 2)'	Todd Nygren of Aerospace Corporation discusses collaborative approaches to detecting, monitoring, and countering threats in space at ASCEND 2023.
JmwoDJD_ReE	'Big changes at Boeing Defense Space & Security'	Ted Colbert on Boeing's defence and space division.

Source: Author's own based on the 44 most relevant videos on space security by YouTube API.

Dr Dmitry Erokhin is a Research Scholar in the Cooperation and Transformative Governance Research Group of the Advancing Systems Analysis Program of the International Institute for Applied Systems Analysis in Laxenburg, Austria. Email: erokhin@iiasa.ac.at.