Satellite Cyber Security Assurance Framework: Assured Unified SPARTA-COSMOS2 Assessment Notation (AUSCAN)

Sam Seo and Jill Slay
School of Computer Science and Information Technology, College of Engineering and Information Technology, Adelaide University, Mawson Lakes, Australia

Sam.Seo@adelaide.edu.au
Jill.Slay@adelaide.edu.au

Abstract: Satellite systems present unique cyber security challenges that distinguish them from conventional IT infrastructure. Once deployed, physical intervention is virtually impossible, leaving operators unable to patch, repair, or replace compromised hardware in orbit. These systems operate under severe constraints in power, processing capability, and bandwidth, limiting the complexity of onboard security measures. Furthermore, the growing integration of commercial off-the-shelf components and IP-based networking has significantly expanded the attack surface, while the increasing dependence of critical sectors on space-based assets has elevated the consequences of a successful attack. Despite these unique risk characteristics, current assessment approaches often treat space systems as standard IT networks, failing to account for the architectural context in which threats occur. Existing cyber security frameworks address either threat identification or architectural classification, but not both simultaneously. SPARTA provides a comprehensive taxonomy of space-specific Tactics, Techniques, and Procedures (TTPs), while COSMOS2 defines the architectural segments of space missions. However, no standardised method currently exists to quantify risk at the intersection of these two frameworks. To address this gap, this paper proposes AUSCAN (Assured Unified SPARTA-COSMOS2 Assessment Notation), a quantitative, segment-aware risk assessment framework. AUSCAN synthesises SPARTA's threat intelligence with COSMOS2's architectural segmentation and applies NIST FIPS 199 impact standards to assign criticality weights to each mission segment. The resulting risk scores are aligned with NASA NPR 8000.4C governance directives to enable actionable decision-making. A hypothetical Ground Segment command injection scenario is used to validate the framework. The results demonstrate that AUSCAN effectively quantifies the impact of security control maturity on risk, reducing the score from 38.4 (Medium/Yellow) to 9.6 (Low/Green) when verified mitigations are applied. This research makes three contributions to space cyber security. First, it establishes a quantitative methodology that integrates SPARTA threat intelligence with COSMOS2 architectural segmentation, grounded in NIST FIPS 199 impact standards. Second, it introduces segment-aware risk scoring, ensuring that identical threats are assessed differently depending on whether they target a recoverable ground station or an irrecoverable satellite. Third, through the inclusion of dynamic vulnerability factors, the framework is adaptable to missions with varying criticality profiles and risk appetites.

Keywords: AUSCAN, SPARTA, COSMOS2, Satellite cyber security, Space risk assessment, Mission assurance

1. Introduction

Space systems provide critical communications, scientific, and national security services globally, with industries spanning banking, logistics, defence, agriculture, and communications now heavily dependent on space-based assets (Akande et al., 2023, Kang et al., 2018). As of 2024, over 11,000 satellites were operating in orbit, driven by the affordability of launch and increased private sector engagement in satellite manufacturing and commercialisation (Jones et al., 2025). This growing dependence makes space a contested environment, where the convergence of space and cyber domains creates attack vectors capable of denying and disrupting critical services including Intelligence, Surveillance and Reconnaissance (ISR) and Position, Navigation and Timing (PNT) (Harrison et al., 2020).

The cyber threat to space systems is growing and evolving, as demonstrated by the 2022 cyberattack on Viasat's KA-SAT network (Boschetti et al., 2022). Nation states are developing jamming, cyberspace capabilities, directed energy weapons, and ground-based anti-satellite capabilities (Defense Intelligence Agency, 2019). Cyber-attacks can target the entire end-to-end space system, ranging from space vehicles and communication links to ground stations and integrated terrestrial networks (Pavur and Martinovic, 2020). The increasing use of Commercial-Off-The-Shelf (COTS) hardware and IP-based networking on Low Earth Orbit (LEO) satellites has significantly expanded this attack surface (Budroweit and Patscheider, 2021). The growth of LEO constellations introduces both inherent resilience and new vulnerabilities that adversaries can exploit at scale (BryceTech, 2025).

Satellite systems present unique challenges that distinguish them from conventional IT infrastructure. Once deployed, physical intervention is virtually impossible, leaving operators unable to patch or replace compromised hardware in orbit (Plotnek and Slay, 2022a). Satellites operate under severe constraints in power, processing capability, and bandwidth, limiting onboard security measures (Falco, 2018). Encryption is

generally only employed between the ground station and the satellite, leaving onboard authentication and data integrity minimal (Banu, 2007, Yue et al., 2023). Existing security approaches in the space domain tend to be isolated, lacking a layered defence-in-depth philosophy (Shahzad et al., 2024, Botezatu, 2024).

Since 2022, the Australian government has recognised these risks by listing space systems as critical infrastructure under the Security of Critical Infrastructure (SOCI) Act (Plotnek and Slay, 2022a). However, despite these unique risk characteristics, current assessment methodologies often treat space systems as standard IT networks, failing to account for architectural segmentation and potentially misidentifying threat severity based on location (Shahzad et al., 2024, Khan et al., 2024, Peled et al., 2023).

Two existing frameworks address aspects of this challenge. The Space Attack Research and Tactic Analysis (SPARTA) framework, modelled after MITRE ATT&CK, provides a comprehensive taxonomy of Tactics, Techniques, and Procedures (TTPs) specific to the space domain (Aerospace Corporation, 2026, Ear et al., 2024). The Compound Space Security (COSMOS2) framework defines five architectural segments, namely Governance, Human, Ground, Space, and Communications, Control and Computing (C3). These segments enable precise asset mapping for security evaluation (Plotnek and Slay, 2022b). However, while SPARTA details what threats exist and COSMOS2 defines what needs protecting, no standardised method currently exists to quantify risk at their intersection.

To address this gap, this paper proposes the Assured Unified SPARTA-COSMOS2 Assessment Notation (AUSCAN), a quantitative, segment-aware risk assessment framework for space cyber security. The research objectives are:

- To develop a quantitative risk assessment methodology that integrates SPARTA's threat intelligence with COSMOS2's architectural segmentation, supported with NIST FIPS 199 impact standards.
- To demonstrate that AUSCAN can differentiate risk severity based on the mission segment, ensuring that identical threats are assessed contextually.
- To validate the framework through a hypothetical case study and align the results with NASA NPR 8000.4C for actionable decisions.

The remainder of this paper is structured as follows. Section 2 reviews background and related work. Section 3 presents the AUSCAN methodology. Section 4 provides a case study and evaluation. Section 5 concludes with contributions and future research directions.

2. Background and Related Work

Historically, space missions relied on physical isolation and limited public knowledge of system architectures as de facto security measures (Abbasi et al., 2025). However, the paradigm has shifted due to the convergence of space technologies with COTS hardware and IP-based networking (Budroweit and Patscheider, 2021, Janicik and Heberle, 2005). These convergences have expanded the cyber-attack surface significantly (Remy and Xu, 2025), with recent studies demonstrating vulnerabilities across multiple segments of the space ecosystem (Plotnek and Slay, 2022b). As space assets become critical to national security and the global economy, standardising cyber security frameworks has moved from theoretical discussion to operational necessity.

Several frameworks have emerged to address this need, each with distinct strengths and limitations.

The SPARTA framework from the Aerospace Corporation addresses the industry-wide lack of space-specific cyber threat intelligence. Modelled after the MITRE ATT&CK framework, SPARTA provides a comprehensive taxonomy of TTPs specific to the space domain (Ear et al., 2024). Its primary strength is the depth and specificity of its threat catalogue, which enables defenders to identify and characterise attack vectors across the space mission lifecycle. However, SPARTA has a notable limitation: it provides detailed information from an attacker's perspective but does not inherently prioritise threats based on the specific architecture of the victim system. A technique is catalogued the same way regardless of whether it targets a ground station or a satellite.

To address architectural ambiguity, the COSMOS2 framework moves beyond the traditional dichotomy of "space vs. ground" segments (Plotnek and Slay, 2022a). Its strength lies in standardising the description of space system architectures by defining five distinct segments: Governance, Human, Ground, Space, and Link (C3), enabling precise asset mapping for risk assessment. However, while COSMOS2 effectively defines what needs to be protected, it does not provide a mechanism to measure how severely a specific threat impacts those segments. It is a descriptive ontology rather than a risk quantification tool.

The integration of threat taxonomies with risk quantification is an emerging field. A notable contribution is the work of Seo and Kim (2025), who proposed a multi-tiered Threat Analysis and Risk Assessment (TARA) framework. Their work demonstrates that SPARTA TTPs can be adapted for quantitative metrics, successfully integrating them to quantify supply chain and infrastructure risks. This represents an important advance in bridging the gap between threat identification and risk measurement. However, their approach focuses primarily on supply chain and defence-in-depth layers and does not explicitly address the architectural segmentation of space missions. Risk is calculated based on the technique (e.g., "How dangerous is malware?") rather than the target segmentation (e.g., "How dangerous is malware on the satellite versus the ground station?").

A clear pattern emerges from this review. SPARTA provides the threat intelligence but lacks architectural context. COSMOS2 provides the architectural context but lacks risk quantification. Seo and Kim's TARA demonstrate quantification is feasible but does not incorporate architectural segmentation. There is currently no standardised metric that weights SPARTA threats according to the COSMOS2 segment they impact. This paper addresses this specific gap by proposing AUSCAN, which applies NIST impact weighting to the COSMOS2 ontology to derive a segment-aware risk assessment score in conjunction with the SPARTA framework.

3. Methodology

AUSCAN is a quantitative assessment notation designed to assess cyber risk in space missions. Unlike traditional risk assessment which usually focus and origin from TTPs, AUSCAN looks from the architecture of the overall space mission. This allow AUSCAN to dynamically adjust the severity of a threat based on the specific segment it targets.

The assessment notation operates by synthesising three variables: Threat Severity (S_{NRS}), Asset Criticality (W_{FIPS}), and Vulnerability Factor (V_f) into the mathematical way to calculate risk at the intersection SPARTA and COSMOS2.

3.1 Threat Severity

Threat Severity quantifies the inherent danger of the attack vector. Utilising SPARTA matrix for TTP identification and adopt the Notional Risk Scores (NRS) methodology proposed by Aerospace Corporation (Seo & Kim 2025). NRS is a tool within SPARTA that helps to provide a baseline for risk assessment for space assets. As there is an overwhelming number of TTP collections in SPARTA, using NRS will reduce the workforce burden by identifying the most mission critical risks (Ear, Bailey & Xu 2024). NRS assign a base risk level to specific techniques based on likelihood and technical impact which is the S_{NRS} variable.

The NRS assigns a base score (0-100) to each SPARTA TTP based on its technical complexity and potential impact. For the purposes of AUSCAN, raw NRS value is utilised. Example: On a high criticality system, a "Flooding" attack to disrupt communications (SPARTA ID EX-0013) has a score of 25; whereas a "Eavesdropping: Active Scanning (RF/Optical)" interference with link by actively transmitting packets to activate the transmitter has a score of 9.

3.2 Asset Criticality

This component quantifies the value or the target asset using COSMOS2 and NIST FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems). COSMOS2 is an ontology which presents segments of space systems in the context of security. The segments are Governance Segment, Human Segment, Ground Segment, Space Segment, Communications, Control & Computing (C3) Segment (Plotnek & Slay 2022b). COSMOS2 when combined with NIST FIPS 199 (Radack 2002), it allows "Critical Value" to be assigned to each segment. FIPS 199 defines three impact levels: Low, Moderate, High which maps to numbers (e.g. 1, 2, 3) to derive an Asset Criticality Weight - W_{FIPS}. See table below.

Table 1: Asset Criticality Weight

COSMOS2 Segment	FIPS 199 Impact Level	Weight	Rationale
Governance	Low	1	Administrative. Attacks here involve policy violations or compliance issues. Possible long-term risk, but no immediate mission failure.
Human	Low	1	Limited range/personnel. Attacks here usually affect data confidentiality (spying) rather than mission critical. Satellite remains safe.

COSMOS2 Segment	FIPS 199 Impact Level	Weight	Rationale
Ground	Moderate	2	Recoverable. Critical for operations but often has redundancy (backup sites) and allows for physical recovery intervention (re-imaging servers).
Space	High	3	Irrecoverable. Impossible physical access to repair. A successful attack here (e.g., de-orbiting) results in total mission loss.
C3	High	3	Critical Path. If the C3 is jammed or compromised, there will be loss of control over satellite, results in total mission loss

The Asset Criticality Weight is assigned to the architecture segment that contain the vulnerability but not necessarily the segment suffering the ultimate consequence. Example will be discussed in the case study section.

3.3 Vulnerability Factor

The third component represent the effectiveness of existing defences. Even a high-severity threat targeting a critical segment poses low risk if sufficient security controls are in place. This is calculated using the "Likelihood of Occurrence" criteria from NIST SP 800-30 Rev. 1 (Appendix G). The "Likelihood of Occurrence" in NIST's guide is the probability that a threat will attempt and successfully exploit a vulnerability, based on threat capability, system exposure, vulnerabilities, and the strength of existing security controls (Fikri et al. 2019). The factor in AUSCAN context represent the probability of a SPARTA TTP bypassing existing controls in COSMOS2 segment. See table below for the quantification of Vulnerability Factor (V_f):

Table 2: Quantification of Vulnerability Factor

NIST Rating	Description (Adapted from SP 800-30 Rev 1)	Vulnerability Factor (V_f)
Very High	No control exists; or controls are incompetent. Attack is almost certain to succeed.	1.0
High	Controls exist but are insufficient or not integrated.	0.8
Moderate	Controls are in place but have known gaps.	0.5
Low	Controls are verified.	0.2
Very Low	Multiple layers of strict controls; exploit is theoretically possible but practically difficult.	0.1

Using Vulnerability Factor is critical as it allows risk assessor to simulate different security controls. It is a coefficient ranging from 0.1 (Secure) to 1.0 (Vulnerable), presenting as multiplication or division depending on the control in place. For example, when encryption is added, V_f drops from 1.0 to 0.2, reducing the total risk score.

3.4 AUSCAN

The final risk score $(Risk_{Total})$ is calculated by the product of the three variables. This multiplicative model present risk is "High" when a dangerous threat targets a critical asset with weak controls. The proposed equation as follows:

$$Risk_{Total} = \sum (S_{NRS} \times W_{FIPS}) \times V_f$$

Where:

S_{NRS} = SPARTA Notional Risk Score of the specific technique used. Range from 1 to 25.

W_{FIPS} = COSMOS2 Weight of the segment being attacked derived from NIST FIPS 199. Range from 1.0 to 3.0.

V_f = Vulnerability Factor is the likelihood of an attack. Range from 0.1 to 1.0.

This formula produces a maximum theoretical risk score of 75 and a minimum of 0.1. To assist in decision-making, the numerical output is aligned with the NASA Risk Management Matrix defined in NASA NPR 8000.4C.

Unlike enterprise IT standards that prioritise data confidentiality, NPR 8000.4C focuses on Safety and Mission Success. This aligns with AUSCAN's targeted assessment domain, which is space asset that has always prioritise safety and mission success. NPR 8000.4C codified the vision of managing risk that threatens space mission and

objectives (Dezfuli et al. 2024). Space agencies and operators utilise the Red-Yellow-Green matrix defined in the NASA Risk Management Handbook, by mapping AUSCAN score to these established tiers, AUSCAN can be directly integrated into existing Continuous Risk Management (CRM) and Risk-Informed Decision Making (RIDM). NPR 8000.4C classified risk based on risk tolerance levels, which is inspired the following tier alignment:

Table 3: AUSCAN Risk Tier

Tier / Colour	AUSCAN Score Range	Risk Definition	Governance Action
High (Red)	51 – 75	Unacceptable	Stop and Fix (T-0 Mitigation). Operations should not procced without immediate mitigation. Acceptance of this risk requires a formal waiver signed by the Program Manager or Control Board.
Medium (Yellow)	25 – 50	Marginal	Plan and monitor. Mitigation resources should be allocated. If immediate mitigation is not possible, risk must be entered into CRM database for tracking and monitor.
Low (Green)	0.1 - 25	Acceptable	Standard Maintenance. Risk is accepted within the standard operational baseline. Standard maintenance and best practices apply.

In NASA context, a "Red" risk represents a threat to Mission Success or Safety of Flight. By setting the threshold for the "High (Red)" at 51, this classification is reserved for scenarios involving high-severity risks against critical space asset, thereby aligning with NASA's comprehensive Safety and Mission Assurance (SMA) processes (Dezfuli et al. 2024). By aligning the quantitative scores with the "Red-Yellow-Green" reporting format used in NPR 8000.4C, AUSCAN provide governance action. Therefore, a score above 51 is not merely a number but serves as a governance action trigger, which should initiate a requirement for Program-level or board-level review. This prevents critical cyber risks from buried in technical logs but a call for actions.

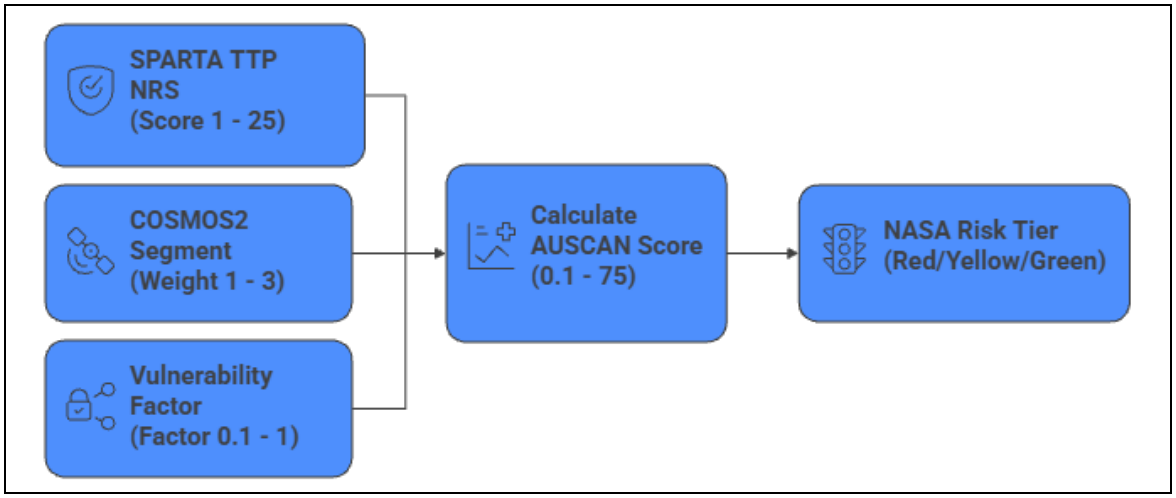

Figure 1: The AUSCAN Process Workflow. This assessment notation synthesised SPARTA and COSMOS2 to derive a quantitative risk score that triggers governance actions

4. Case Study and Evaluation

To validate AUSCAN, this section applies the framework to a hypothetical command injection scenario, demonstrates its sensitivity to architectural context, compares it against technique-only assessment, and discusses limitations.

4.1 Scenario Description

A Low Earth Orbit (LEO) mission architecture consists of a CubeSat constellation control by a ground station. The threat is an external attacker gains unauthorised access to ground station's Command and Control (C2) server and attempts to send a malicious "shutdown" command to the satellite. The mapping with both framework is:

- SPARTA Technique: Modify On-Board Values: Attitude Determination and Control Subsystem. (ID: EX0012.08).

- COSMOS2 Segment: Ground Segment (Attack entry point).

4.2 Variable Assignment

Using the methodology defined in previous section, the following values are assigned to the scenario variables:

1. Risk Severity (S_{NRS}): The attacker is attempting to shut down the satellite.

- Value: 24 (High Severity)
- Rationale: This SPARTA TTP is a direct manipulation of satellite's physical state. NRS of near-maximum score has been assigned by SPARTA.

2. Asset Weight (W_{FIPS}) : The compromised asset is the C2 server in the ground station that communicates with the satellite in space.

- Value: 2.0 (Moderate Impact, per Table 1).
- Rationale: While critical, ground station is physically accessible and can be restored. It is important to note that ground station is where the vulnerability exists and where the mitigation needs to be applied. AUSCAN focus on to bringing out the root cause of the risk where governance action should be taken. Satellite is not weighted as it is not vulnerable in this scenario; it is simply obeying a command. The vulnerability component is the ground station's lack of validation.

3. Vulnerability Factor (V_f) : In this scenario, two states are compared:

- State A (Vulnerable): The C2 server only has single-factor authentication and lack of command signing. Value: 0.8 (Controls exist but are insufficient or not integrated.)
- State B (Mitigated): The C2 server implemented Multi-Factor Authentication (MFA) and cryptographic command validation. Value: 0.2 (Controls are verified.)

4.3 Risk Calculation Results

Applying AUSCAN to both State A and B and the results are as follows:

Table 4: Example Case Study using AUSCAN calculation

State	S_{NRS}	W_{FIPS}	V_f	$Risk_{Total}$	Risk Tier
State A (Vulnerable)	24	2	0.8	38.4	Medium
State B (Mitigated)	24	2	0.2	9.6	Low

The 75% reduction from 38.4 to 9.6 is driven entirely by improved security controls, with threat severity and asset criticality held constant. This demonstrates that AUSCAN can quantify the measurable impact of specific defensive investments.

4.4 Sensitivity Analysis: Segment-Aware Scoring

To validate AUSCAN's architectural sensitivity, the same technique (EX0012.08, S_{NRS}= 24) is applied across all five COSMOS2 segments under identical vulnerability conditions (V_f= 0.8, representing insufficient controls).

Table 5: Sensitivity analysis – same threat across different COSMOS2 segments

COSMOS2 Segment	S_{NRS}	W_{FIPS}	V_f	$Risk_{Total}$	Risk Tier
Governance	24	1	0.8	19.2	Low
Human	24	1	0.8	19.2	Low
Ground	24	2	0.8	38.4	Medium
Space	24	3	0.8	57.6	High
C3	24	3	0.8	57.6	High

A traditional technique-only assessment would assign a single score regardless of target. AUSCAN produces scores ranging from 19.2 to 57.6, which spans across all three risk tiers. This confirms that the framework captures the operational distinction between a recoverable ground station and an irrecoverable space asset.

4.5 Comparative Analysis: AUSCAN vs. Technique-Only Assessment

Table 6: Comparative analysis – technique-only vs. AUSCAN assessment

Approach	Risk Score	Risk Tier	Governance Action
SPARTA NRS only	24	N/A (no tier mapping)	No defined action
AUSCAN — Ground (State A)	38.4	Medium	Plan and monitor
AUSCAN — Space (State A)	57.6	High	Stop and fix

Without AUSCAN, a score of 24 provides no architectural context, no vulnerability adjustment, and no governance action mapping. AUSCAN resolves this by producing contextualised scores linked to NASA NPR 8000.4C response tiers (Dezfuli et al., 2024).

4.6 Limitations

Two key limitations must be acknowledged. First, the case study is hypothetical. Although variable assignments are grounded in established standards, the framework has not yet been validated against operational data from a real-world mission. Second, AUSCAN currently evaluates threats individually. In practice, space missions face compound threats where multiple TTPs may be executed simultaneously, and the current formula does not model cascading risks (Remy and Xu, 2025).

5. Conclusion and Future Work

5.1 Summary

As space systems transition from isolated legacy architectures to networked ecosystems, the need for cyber security frameworks that account for both threat intelligence and mission architecture has become urgent. This paper addressed the gap between threat-focused frameworks such as SPARTA and architecture-focused ontologies such as COSMOS2 by proposing AUSCAN (Assured Unified SPARTA-COSMOS2 Assessment Notation), a quantitative, segment-aware risk assessment framework for space cyber security.

The AUSCAN methodology synthesises three variables – Threat Severity derived from SPARTA's Notional Risk Scores, Asset Criticality derived from COSMOS2 segments weighted using NIST FIPS 199, and a Vulnerability Factor adapted from NIST SP 800-30 – into a single risk score mapped to NASA NPR 8000.4C governance tiers.

5.2 Key Findings

The framework was validated through a hypothetical Ground Segment command injection scenario. Three key findings emerged from the evaluation:

First, AUSCAN demonstrated sensitivity to security control maturity. The implementation of verified controls (MFA and cryptographic command validation) reduced the risk score from 38.4 (Medium/Yellow) to 9.6 (Low/Green), representing a 75% reduction. This confirms that the framework can quantify the measurable impact of specific defensive investments.

Second, the sensitivity analysis confirmed that AUSCAN produces architecturally meaningful distinctions. The same SPARTA technique applied across all five COSMOS2 segments generated scores ranging from 19.2 (Low) to 57.6 (High), spanning all three risk tiers. This validates the core claim that identical threats should be assessed differently depending on where in the mission architecture they occur.

Third, the comparative analysis demonstrated that without segment-aware scoring, a technique-only assessment provides no architectural context, no vulnerability adjustment, and no mapping to governance actions. This would have left mission directors without a standardised basis for decision-making.

5.3 Contributions

This research makes three contributions to the field of space cyber security:

- Methodological Integration: AUSCAN establishes, to the authors' knowledge, the first quantitative methodology that integrates SPARTA threat intelligence with COSMOS2 architectural segmentation. By grounding the framework in established standards (NIST FIPS 199 and NASA NPR 8000.4C), it ensures compatibility with existing governance processes including Continuous Risk Management (CRM) and Risk-Informed Decision Making (RIDM).

- Architectural Context: The use of COSMOS2 segmentation ensures that risk scores reflect the operational reality of space missions. The sensitivity analysis confirmed that a vulnerability in a recoverable ground station (score: 38.4) is assessed differently from the same vulnerability in an irrecoverable space asset (score: 57.6), directly addressing the limitation of technique-only approaches identified in prior work (Shahzad et al., 2024, Seo and Kim, 2025).
- Mission Adaptability: Through the inclusion of dynamic vulnerability factors, AUSCAN can be tailored to missions with varying criticality profiles and risk appetites. The framework's variables are modular, allowing mission-specific customisation of segment weights and vulnerability assessments without altering the underlying methodology.

5.4 Implications for Practice

The practical significance of AUSCAN extends beyond academic contribution. For mission directors and space system operators, AUSCAN provides a structured mechanism to translate technical cyber threats into governance actions. The alignment with NASA's Red-Yellow-Green reporting format means that AUSCAN outputs can be integrated directly into existing risk reporting workflows without requiring new governance infrastructure. For the Australian context specifically, where space systems are now classified as critical infrastructure under the SOCI Act, AUSCAN offers a potential pathway for standardising cyber security risk assessment across the growing Australian space industry.

5.5 Future Work

Several concrete avenues for future research have been identified:

- Real-World Validation: The immediate priority is to apply AUSCAN to operational data from a real-world CubeSat mission, working with industry partners to validate the framework against actual threat scenarios, security architectures, and operational risk tolerances. This will test whether the fixed FIPS 199 segment weights hold across different mission types or require mission-specific calibration.
- Software Prototype and Automation: A software tool that ingests live data feeds from C2 systems and vulnerability scanners to calculate AUSCAN scores in real-time would transform the framework from a manual assessment tool into a live cyber-risk dashboard for Mission Control. This prototype should include automated alert triggering based on risk tier thresholds.
- Digital Twin Integration: Connecting the AUSCAN software prototype to a digital twin of a satellite mission would enable predictive risk forecasting, allowing operators to simulate the impact of emerging threats or proposed security control changes before they are implemented in the operational environment.

5.6 Closing Remarks

As the global reliance on space-based services continues to grow and the cyber threat landscape evolves, the need for rigorous, architecture-aware risk assessment in space cyber security will only intensify. AUSCAN represents a step toward bridging the gap between threat intelligence and mission assurance governance, providing a standardised notation that translates technical cyber risks into actionable decisions. By unifying the strengths of SPARTA and COSMOS2 within a quantitative framework aligned with established aerospace governance standards, this work offers a foundation upon which the space cyber security community can build more resilient and assured space missions.

Ethic Declaration: This research does not involve human participants, human data, or animal subjects. Accordingly, ethical approval was not required for this study under the relevant institutional and national guidelines. The authors confirm that the research was conducted in accordance with principles of research integrity and responsible research practice.

AI Declaration: The authors used AI-based tools (e.g., Gemini) solely to assist with proofreading. In addition, Napkin AI was used to generate figure-1 based on author-provided concepts and descriptions. The AI tools did not contribute to the research design, data analysis, or interpretation of results. All intellectual contributions and responsibility for the content remain with the authors.

References

Abbasi, A., Falco, G. J., Fischer, D. & Slay, J. (2025) "Guardians of the Galaxy: Protecting Space Systems from Cyber Threats (Dagstuhl Seminar 25101)". Dagstuhl Reports, 15(3), 1-38.

Aerospace Corporation (2026) Space Attack Research & Tactic Analysis (SPARTA), 2026. Available online: https://sparta.aerospace.org/ [Accessed.

Akande, A. J., Foo, E., Hou, Z. & Li, Q. (2023) Cybersecurity for Satellite Smart Critical Infrastructure, in Pal, S., Jadidi, Z., Foo, E. & Mukhopadhyay, S. C. (eds), Emerging Smart Technologies for Critical Infrastructure. Cham: Springer Nature Switzerland, 1-22.

Banu, P. S. R. (2007) Satellite on-board encryptionUniversity of Surrey (United Kingdom).

Boschetti, N., Gordon, N. G. & Falco, G. (2022) Space cybersecurity lessons learned from the viasat cyberattack, ASCEND 2022, 4380.

Botezatu, U.-E. (2024) "Space cybersecurity: a survey of vulnerabilities and threats". Romanian Cyber Security Journal, 6(2), 53-60.

BryceTech (2025) Global Orbital Space Launches Q3 2025BryceTech.

Budroweit, J. & Patscheider, H. (2021) "Risk Assessment for the Use of COTS Devices in Space Systems under Consideration of Radiation Effects". Electronics, 10(9), 1008.

Defense Intelligence Agency (2019) Challenges To Security in Space.

Dezfuli, H., Guarro, S., Everett, C., Benjamin, A. & Skow, M. C. (2024) NASA Risk Management Handbook: Version 2.0, Part 1.

Ear, E., Bailey, B. & Xu, S. (2024) "Towards principled risk scores for space cyber risk management". arXiv preprint arXiv:2402.02635.

Falco, G. (2018) The vacuum of space cyber security, 2018 AIAA SPACE and Astronautics Forum and Exposition.

Fikri, M. A., Putra, F. A., Suryanto, Y. & Ramli, K. (2019) "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency". Procedia Computer Science, 161, 1206-1215.

Harrison, T., Johnson, K., Moye, J. & Young, M. (2020) Space threat assessment 2020Center for Strategic and International Studies (CSIS).

Janicik, J. & Heberle, J. (2005) "Internet Protocol (IP) as a Standard for Command and Control of Satellites".

Jones, K. L., Dhopade, P. & DeMarchi, L. (2025) Spaceportopia: Global trends in orbital launch and satellite deploymentCorporation, A.

Kang, M., Hopkinson, K., Betances, A. & Reith, M. (2018) Mitigation of cyber warfare in space through Reed Solomon codes, Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018.

Khan, S. K., Shiwakoti, N., Diro, A., Molla, A., Gondal, I. & Warren, M. (2024) "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions". International Journal of Critical Infrastructure Protection, 47, 100724.

National Institute of Standards and Technology (2004) 199:2004: Standards for security categorization of federal information and information systems.FIPS Publication 199.

Pavur, J. & Martinovic, I. (2020) "Sok: Building a launchpad for impactful satellite cyber-security research". arXiv preprint arXiv:2010.10872.

Peled, R., Aizikovich, E., Habler, E., Elovici, Y. & Shabtai, A. (2023) "Evaluating the security of satellite systems". arXiv preprint arXiv:2312.01330.

Plotnek, J. & Slay, J. (2022a) New dawn for space security, International Conference on Cyber Warfare and Security. Academic Conferences International Limited.

Plotnek, J. & Slay, J. (2022b) "Space Systems Security

A Definition and Knowledge Domain for the Contemporary Context". Journal of Information Warfare, 21(3), 103-119.

Remy, J. L. C. & Xu, S. (2025) "Towards a Systematic Taxonomy of Attacks against Space Infrastructures". arXiv preprint arXiv:2512.12829.

Seo, S. & Kim, D. (2025) "Multi-tiered space cyber TARA: Quantification of risk and mitigation with SPARTA TTP".

Shahzad, S., Joiner, K., Qiao, L., Deane, F. & Plested, J. (2024) "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers". Systems, 12(10), 434.

Yue, P., An, J., Zhang, J., Ye, J., Pan, G., Wang, S., Xiao, P. & Hanzo, L. (2023) "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead". IEEE Communications Surveys & Tutorials, 25(3), 1604-1652.