Systematically Integrating Cyber Threat Intelligence into Resilient Space-Cyber Architectures

Chathura Abeydeera
University of Adelaide, Australia

ch@hura.au

Abstract: Space systems are undergoing unprecedented commercialisation, increased autonomy and expanded connectivity, bringing both operational efficiency and heightened exposure to evolving cyber threats. These systems underpin critical services such as communication, navigation and Earth observation, yet their cybersecurity practices remain inconsistent across the global space ecosystem. Although frameworks such as NIST SP 800-160, NASA-STD-1006, ECSS-Q-ST-80C and MITRE's Cyber Resiliency Engineering Framework (CREF) provide guidance for secure engineering, they lack mechanisms for the systematic integration of Cyber Threat Intelligence (CTI). This paper examines current CTI integration practices and the organisational, technical, and regulatory barriers that hinder CTI-informed resilience in space-cyber architectures. Drawing upon an extensive review of academic and industry literature, the study maps how CTI is currently applied across space-system lifecycles and identifies critical impediments to broader adoption. The findings reveal that CTI is primarily leveraged in an ad hoc, reactive manner for patching and advisory processes, with minimal integration into design or operations. Identified barriers include fragmented standards, limited automation in threat-intelligence consumption, cultural resistance to information sharing and divergent regulatory frameworks across jurisdictions. The paper concludes with analytical insights into how these findings can inform future policy and research directions aimed at improving intelligence-driven resilience within the space sector.

Keywords: Cyber threat intelligence, Space-cyber architecture

1. Introduction

As space operations expand to support defence, communications, and scientific missions; the cyber threat landscape surrounding them has become increasingly complex. The convergence of terrestrial networks with orbital assets introduces additional vulnerabilities through shared infrastructure, COTS components and cloud-integrated mission systems (Falco, 2019; Bradbury et al., 2020). Although many national agencies and commercial operators implement baseline controls aligned to NIST, ECSS or NASA standards, few operationalise CTI as part of system design or mission assurance.

This paper addresses two central questions.

What are the current practices for integrating CTI into the cybersecurity of space systems?

What organisational, technical and regulatory barriers impede CTI-informed resilience in space cyber architectures?

Through addressing these questions, the paper aims proposes a pathway for transforming CTI from a predominantly reactive function into a proactive design and governance instrument for the space sector.

2. Space Architecture Overview

Space system architecture consists of a tightly interconnected ecosystem spanning the ground, link, space, user, and integration domains. Each domain contains distinct components, services and operational functions that collectively contribute mission assurance. The architectural model, as illustrated in the referenced diagram produced by the IEEE P3536 - Space System Cybersecurity Design Standard Working Group demonstrates that cyber risk in space systems emerges not from isolated components but from the interactions and dependencies among these domains (Willbold et al., 2023, Bradbury et al., 2020).

The ground segment includes mission control centres, launch operations, science data systems and the ground security operations centre (GSOC). Key functions include telemetry and telecommand (TM/TC) operations, payload tasking, mission scheduling, data processing, intrusion detection and vulnerability management. Ground stations and associated network services act as the operational anchor for space assets, creating a high-value target for adversaries due to their central role in command and control (Peled et al., 2023).

The link segment encompasses all communication pathways between ground and space components, including RF links, optical links, data uplinks and downlinks, modulation and demodulation functions, radio resource management and error correcting protocols. This segment represents a critical attack surface, as adversaries may exploit weak authentication, unencrypted channels, or disruption techniques such as jamming and spoofing

(Tedeschi, 2022). Link-level monitoring and anomaly detection are increasingly recognised as essential resilience measures.

The space segment consists of the satellite bus and payload. The bus includes subsystems such as CDHS, cryptographic services, ADCS/GNCS, propulsion, power systems, data storage and communication modules. These components support satellite health, stability, and communication. The payload provides mission-specific capabilities such as scientific instruments or imaging systems and inter satellite links. The space segment is resource constrained, physically inaccessible post launch and therefore highly sensitive to pre-launch supply chain risks and firmware integrity failures (Varadharajan & Suri, 2022).

The user segment includes components such as VSAT terminals, GNSS receivers, PNT systems, anomaly detection tools for user-space threats, and encryption/decryption services used by downstream consumers. User terminals often form the outermost and least controlled attack surface, introducing risks through social engineering, misconfiguration, weak authentication or exploitation of unpatched end user equipment (Casaril, F. et al. 2024; CISC, 2024).

The integration layer spans the cross cutting functions that link all segments together, including key management, PKI, intrusion and anomaly detection, software testing and emulation, threat intelligence, supply chain management, and system wide situational awareness. This layer is essential for cyber resilience, as it governs the consistency and coherence of security practices across the entire architecture (Falco et al., 2024).

Taken together, this architectural model highlights the multidimensional attack surface across space systems. It shows that cyber threats do not target components in isolation. Rather, adversaries exploit interdependencies between ground stations and satellites, link protocols and bus subsystems, and user devices and payload data flows. These interactions emphasise the need for a holistic understanding of space architecture to inform CTI integration and resilience planning.

3. Space Infrastructure and Criticality

Space infrastructure underpins a broad array of terrestrial and orbital services, spanning communications, remote sensing, meteorology, navigation, scientific experimentation, financial-timing and national security functions. The criticality of these services extends far beyond the space sector itself, embedding orbital systems deeply into the operational fabric of modern societies (Plotnek, J. J., & Slay, J. (2022; Bradbury et al., 2020). As a result, the resilience of space systems is no longer a specialised engineering concern but a strategic national priority.

Sectors such as aviation, maritime logistics, agriculture, emergency services and financial markets rely on satellite-enabled Positioning, Navigation and Timing (PNT), GNSS integrity, continuous communications, and Earth observation data. Interruptions to these services can lead to cascading failures across essential national systems. This interdependence elevates space systems from mission-specific platforms to indispensable components of national critical infrastructure ecosystems.

The strategic value of space infrastructure is amplified by increasing geopolitical contestation. Satellites now function as both military enablers and potential strategic targets, providing reconnaissance, missile warning, secure communications, and situational awareness (Tedeschi et al., 2022). In this context, cyber threats become attractive because they offer a means to disrupt, degrade, or manipulate services without the visibility or escalation risk of kinetic attacks. This geopolitical environment intensifies the need for intelligence-driven cyber resilience.

While countries such as Australia, the United Kingdom and several in the European Union have begun to explicitly recognise space services as critical infrastructure, others including the United States have not fully codified space within CI legislation, instead emphasising sector-specific voluntary guidance (Vasquez, 2024). The absence of a harmonised global classification framework leads to inconsistent baseline security requirements, non-uniform reporting obligations, and uneven incentives for CTI sharing. This fragmentation inhibits collective threat awareness and slows incident coordination.

The NewSpace environment, characterised by rapid growth in commercial operators, launch providers, subsystem vendors, and downstream service integrators, has expanded the global supply chain significantly (Vollmer, 2021). Commercial operators often enter the market with limited cybersecurity maturity and minimal regulatory oversight. As a result,

- Heterogeneous supply chains create opportunities for covert manipulation of firmware, components and software.
- Varied security practices across integrators increase systemic exposure
- Dependency on commercial ground stations and cloud integrated architectures expands the threat surface (Varadharajan & Suri, 2022)

These supply chain interdependencies mean that vulnerabilities in one noncritical component can exploited and propagate across mission systems or even across operator networks, reinforcing the need for sector-wide CTI coordination.

Unlike terrestrial systems, space assets suffer unique fragility. Once launched, hardware cannot be physically accessed, components cannot be replaced, and compromise events, whether via malicious telecommands, payload manipulation or firmware tampering may be irreversible (Peled et al., 2023). This amplifies the importance of early threat awareness, supply chain assurance, and mission-specific intelligence, making CTI indispensable at design, integration and ground operations phases. The 2022 cyberattack against Viasat's KA-SAT network during the onset of the Russia-Ukraine conflict illustrates this fragility vividly. Destructive interference against ground side modems cascaded into widespread service disruption across Europe, demonstrating how targeted cyber operations can produce rapid, large-scale, and operationally irreversible impacts on satellite-enabled services (Boschetti et al., 2023)

These factors collectively show that space systems occupy a unique position within global critical infrastructure. Their geopolitical sensitivity, operational irreversibility, commercial heterogeneity and multi-sectoral dependencies demand a more structured and intelligence-driven approach to cyber resilience. CTI becomes essential not merely for operational monitoring but for informing architecture decisions, prioritising vulnerabilities, contextualising adversary intent, and aligning cross-operator understanding of cyber risks. Recognising space as critical infrastructure, formally and practically, is therefore a foundational step toward enabling effective CTI-informed resilience.

4. Security Posture and Trends

Space assets are exposed to a diverse threat set, including RF jamming, spoofing, supply-chain tampering, and software exploitation (Tedeschi et al., 2022). The emergence of NewSpace has introduced thousands of small satellites built with commercial components, expanding the potential attack surface (Vollmer, 2021). While COTS adoption accelerates innovation, it imports known vulnerabilities into orbit (Varadharajan & Suri, 2022). Post-launch patching limitations make preemptive, CTI-driven hardening indispensable. Frameworks such as IEEE P3349 seek to codify baseline controls but stop short of defining CTI workflows (Falco et al., 2024).

The security posture of contemporary space systems reflects a convergence of legacy assumptions, rapidly evolving threat-actor capabilities, and structural changes in how space services are designed, launched, and operated. Historically, satellite systems were engineered under the implicit assumption of isolation and physical security; orbital distance and specialised protocols were believed to offer inherent protection (Livingstone & Lewis, 2016). These assumptions no longer hold in the NewSpace era, where increased interconnectivity, commercialisation, software-defined architectures, and cloud-integrated mission systems have expanded the exposure of space infrastructure to cyber threats.

Nation-state and state-aligned groups increasingly view space infrastructure as a strategic cyber target due to its geopolitical significance and the potential for creating widespread disruption without kinetic escalation (Tedeschi et al., 2022). Operations attributed to groups such as Russian state APT demonstrate that satellite-enabled services including broadband connectivity, military communications, and critical civilian infrastructure are viable and attractive targets. This shift has demonstrated the real-world consequences of targeting space-reliant networks, including the potential for widespread service disruption, operational degradation and downstream impacts on civilian and military systems.

The proliferation of small satellites, CubeSat constellations, private launch providers, and space-as-a-service models has diversified the operational landscape. Commercial entrants often lack the longstanding cybersecurity culture found in national space agencies (Pavur & Martinovic, 2022). Variability in vendor maturity creates uneven security baselines across the supply chain, from firmware development to ground operations. This heterogeneity presents systemic risks; the compromise of a single insecure commercial subsystem can propagate across integrated mission environments.

The increasing reliance on commercial off-the-shelf (COTS) components, virtualised ground stations, and cloud-based mission management platforms accelerates innovation and development but introduces familiar IT vulnerabilities into space systems (Varadharajan & Suri, 2022). Publicly documented architectures and firmware interfaces allow threat actors to discover, replicate, and weaponise vulnerabilities pre-launch. Once deployed, patching constraints such as limited uplink bandwidth, operational risks, and strict mission schedules make remediation slow and resource intensive.

Modern satellites increasingly rely on software-defined radios (SDRs), reprogrammable payloads, and flexible bus architectures that can be updated or reconfigured on orbit. While these capabilities enhance mission agility, they also widen the attack surface. Vulnerabilities in update mechanisms, command authentication, or cryptographic key management can enable adversaries to alter payload behaviour or interfere with mission data (Saha et al., 2019).

Ground stations, satellite operations centres, cloud-based TT&C pipelines, and data distribution platforms now form essential components of end-to-end mission architecture (Peled et al., 2023). This creates shared dependencies between terrestrial and orbital systems, making ground nodes attractive targets for attackers seeking scalable impacts. The KA-SAT incident again illustrates how ground-side compromise can cascade into large-scale space service disruption.

The Internet of Space Things (IoST), where satellites, sensors, user devices, and terrestrial systems interact, creates a distributed cyber-physical ecosystem with multiple entry points (Falco, 2019). The growing volume of inter-satellite links, automated crosslink routing, and mesh style constellations increases the complexity of securing communications, trust boundaries, and identity management.

These trends highlight a widening gap between threat-actor capabilities and the current maturity of space cybersecurity practices. The increasingly contested and interconnected nature of the space environment demands not just stronger controls but the ability to continuously update assumptions, detect novel behaviours, and understand adversary motivations. CTI becomes critical to bridging this gap by providing the contextual, adaptive insight needed to interpret evolving attack patterns, prioritise risks, and respond proactively.

5. Cybersecurity Standards and CTI Relevance

Cybersecurity guidance for space systems is shaped largely by terrestrial security engineering frameworks that have been adapted, sometimes only partially, to the unique constraints of orbital environments. While these standards provide essential foundations for secure design, assurance, and operational governance, they vary considerably in scope, maturity, and applicability to space architectures. Importantly, none of the major frameworks currently offer explicit mechanisms for the systematic integration of Cyber Threat Intelligence (CTI), leaving operators to independently interpret how intelligence should inform their engineering, monitoring, and incident-response processes.

A review of existing standards highlights several systemic themes that shape their effectiveness and limitations in supporting intelligence-informed resilience.

- Space operators often adopt a blend of NASA, ESA/ECSS, NIST, or defence-specific overlays depending on contractual obligations, launch location, or vendor preferences. This leads to inconsistent baselines and divergent interpretations of security requirements, complicating cross-operator CTI sharing and coordinated defence activities (Falco et al., 2024) creating a fragmentation of security expectations across jurisdictions and mission types.
- Most standards focus on secure design, testing, and verification, but provide limited guidance on how evolving adversary behaviours should influence ongoing risk assessments, threat modelling, or detection engineering. This is particularly problematic given the dynamic nature of threats against space systems (Kavallieratos & Katsikas, 2023).
- While frameworks outline high-level requirements for monitoring and incident response, they provide limited guidance on how CTI should shape operational telemetry design, anomaly detection logic, cross-segment correlation, and mission-specific threat prioritisation. This lack of integration mechanisms results in reactive rather than intelligence-led security postures.

Against this backdrop, the following table summarises how major space and cybersecurity standards address CTI, or fail to, and highlights the gaps that continue to limit intelligence-informed resilience across the sector.

Table 1: Summary of major space and cybersecurity standards address CTI

Standard / Framework	Primary Focus	CTI Inclusion	Key Gaps
NASA-STD-1006	Space system protection from physical and cyber threats	Absent	No mechanism for threat data ingestion or intelligence-led control design
ECSS-Q-ST-80C	Software product assurance	Absent	Static assurance lacking adaptive intelligence feedback
NIST SP 800-160	Systems security engineering	Partial	Lacks space-specific tailoring and CTI implementation detail
MITRE CREF	Cyber resiliency for critical systems	Implicit	Limited guidance on CTI integration and telemetry mapping
IEEE P3349	Space system cybersecurity trustworthiness	Emerging	Focused on component hardening, minimal CTI automation guidance

6. Literature Synthesis: Threats and CTI Use in Space

The literature shows that cyber threats to space systems arise from a combination of architectural complexity, evolving adversary sophistication, and the persistent integration of terrestrial technologies into orbital environments. Unlike traditional IT systems, space systems involve interdependent segments: ground, link, space, user, and integration layers. Each with distinct threat vectors but also tightly coupled behaviours. The literature consistently highlights three overarching realities:

- Adversaries increasingly target cross-segment dependencies
- Vulnerabilities are frequently introduced long before launch through the supply chain, and
- CTI remains underutilised despite its potential to inform both design and operational defence.

The literature consistently structures threats across control, component, and interface layers, reflecting how adversaries exploit weaknesses not in isolation but along pathways that traverse multiple architectural boundaries.

Research documents Control Layer Threats involving manipulation of telecommands, uplink interference, unauthorised tasking, and degradation of command authority (Bradbury et al., 2020). Attacks at this layer can cause loss of mission control, orbital manoeuvre disruption, or payload misuse. These threats often stem from insufficient authentication, outdated cryptographic implementations, or misconfigured TC interfaces.

Vulnerabilities within satellite buses, payload firmware, and subsystems have been revealed through empirical studies, including experimental security analyses of in-orbit satellites (Willbold et al., 2023). Supply-chain compromise, hardware Trojans, and unauthorised firmware modifications remain critical vectors. The literature emphasises that these Component Layer Threats often originate pre-launch through inadequate assurance processes or opaque vendor components (Varadharajan & Suri, 2022).

Weaknesses in TM/TC links, inter-satellite links, ground-station networks, and cloud-based mission architectures expose systems to Interface Layer Threats such as jamming, spoofing, replay attacks, network intrusion and session hijacking (Peled et al., 2023). With increasing reliance on standardised IP based protocols, attackers are able to adapt known terrestrial attack patterns to space-ground interfaces.

Across all layers, the attack surface has expanded due to IoST, mesh constellations, and software-defined architectures, allowing adversaries to exploit vulnerabilities dynamically across segments.

The following visual threat taxonomy table consolidates threats across architectural layers, synthesising insights from Bradbury et al. (2020), Willbold et al. (2023), Varadharajan & Suri (2022), and Peled et al. (2023). It provides a structured basis for comparing adversary behaviours and identifying CTI-relevant intelligence requirements.

Table 2: Threat Taxonomy Across Architectural Layers

Architectural Layer	Threat Category	Description	Representative Adversary Techniques	CTI-Relevant Intelligence
Control Layer	Telecommand Manipulation	Injection or modification of TC frames to alter spacecraft state or payload activity	Replay attacks, brute-force TC guessing, protocol exploitation	Actor TTPs targeting TM/TC paths; protocol abuse cases; command-set intelligence
Control Layer	Uplink/Downlink Interference	Jamming, spoofing, or signal distortion affecting mission operations	RF jamming, GNSS spoofing, downlink noise flooding	RF threat signatures; geolocation of repeat interference events
Component Layer	Firmware/Payload Tampering	Modification of bus or payload firmware pre- or post-launch	Supply-chain compromise, malicious firmware injection	Supplier intelligence; SBOM-linked CVEs; firmware behavioural baselines
Component Layer	Hardware Trojans	Embedded malicious logic in chips/subsystems	Rogue chip activation, side-channel manipulation	Supply-chain provenance intel; vendor risk profiles
Interface Layer	Ground–Space Link Exploitation	Attacks against TM/TC links, inter-satellite links, or ground–cloud interfaces	Session hijacking, protocol downgrade, MITM attacks	Network-level IoCs; link-layer anomaly indicators
Interface Layer	Ground Segment Intrusion	Compromise of GS networks, SOC systems, cloud mission pipelines	Credential theft, lateral movement, privilege escalation	Campaign intelligence; intrusion-set profiles
User Layer	Terminal Exploitation	Abuse of end-user devices (e.g., VSATs, GNSS units) to degrade or manipulate mission outputs	Modem compromise, user-equipment spoofing	IoT/VSAT threat intel; malware signatures
Integration Layer	PKI/Key Management Compromise	Abuse or leakage of cryptographic keys used across segments	Key extraction, certificate forgery	Crypto-related CTI; key-compromise reports
Integration Layer	Supply-Chain Subversion	Manipulation of components, software, or services during development/production	Counterfeit parts, malicious dependencies	Upstream vendor intelligence; ecosystem monitoring

The literature also identifies a spectrum of adversaries, nation-states, state proxies, criminal groups, hacktivists, and insiders, each motivated by espionage, disruption, competitive advantage, coercion, or opportunism (Maple et al., 2020). Threat actors are also shifting toward campaign-based operations, using long-term intrusion life cycles (Hutchins et al., 2011). These campaigns frequently involve,

- supply-chain infiltration
- credential harvesting across vendor networks
- lateral movement through ground segment infrastructure
- manipulation of command paths or space-ground interfaces

The literature warns that persistent access to any one segment, particularly the integration segment, can allow threat actors to stage complex, multi-step attacks affecting orbital assets.

Despite the breadth of threats, the role of CTI in space cybersecurity remains limited and inconsistent. Current CTI use can be grouped into three domains:

- Design-Time CTI Use: CTI is informally used to identify high-risk components, known vulnerabilities, and adversary TTPs relevant to system architecture. However, there is little evidence of structured processes that integrate CTI directly into threat modelling, requirements engineering, or interface design (Falco et al., 2024). Most CTI inputs occur at late design stages, reducing their value.
- Run-Time CTI Use: Operators primarily use CTI in the form of advisories, IoCs, and vulnerability alerts for patching and defensive monitoring. There is minimal automation linking CTI to detection logic, telemetry schemas, or satellite-specific anomaly-detection baselines (Kavallieratos & Katsikas, 2023). Cloud-integrated ground operations offer more opportunities for CTI-driven detection, but adoption remains inconsistent.
- Governance and Sharing: Space ISACs and cross-agency intelligence exchanges exist but face constraints due to classification regimes, liability concerns, and uneven maturity across participants (Plotnek, J. J., & Slay, J. 2022). These cultural and structural barriers restrict intelligence flow, undermining the collective situational awareness required for resilience.

Across literature, several recurring gaps emerge:

- Lack of structured CTI intake methods for system engineering, interface hardening, or requirements validation.
- Absence of space-specific threat taxonomies that organise adversary behaviours, attack vectors, and segment-specific vulnerabilities.
- Limited integration of CTI into threat modelling tools and architectural patterns used by operators.
- Operational silos limiting intelligence sharing, particularly between commercial and government operators.
- Insufficient automation linking CTI ingestion to configuration updates, detection logic or anomaly models.

Overall, the literature points to a widening gap between the speed and sophistication of space-targeting adversaries and the static, highly manual nature of CTI use in the sector. Although CTI has the potential to significantly strengthen resilience by anticipating adversary behaviour, informing architectural decisions, and enhancing anomaly detection. It is not yet embedded into space system lifecycles in a systematic or measurable manner. This synthesis highlights the need for deeper investigation into CTI integration practices and the barriers currently limiting intelligence-informed resilience.

7. Current Practices

Across the literature and industry reporting, current CTI integration practices in space systems remain fragmented, uneven, and primarily reactive. While operators increasingly acknowledge the value of intelligence-informed defence, the practical application of CTI differs substantially across mission types, organisational structures, and maturity levels. Several themes recur across empirical studies and technical analyses, highlighting how CTI is currently used and where gaps persist.

Most operators employ CTI to support patching cycles, vulnerability scanning, and exposure assessments. Intelligence feeds (e.g., CVEs, vendor bulletins, ISAC alerts) assist in identifying weaknesses in ground infrastructure, cloud platforms, commercial software, and third-party services (Ettinger, 2019; Borges Amaro et al., 2022). However, CTI is rarely embedded into requirements engineering, design reviews, interface assessments, or system-level hazard analyses. As noted by Falco et al. (2024), this results in CTI influencing operational posture but seldom shaping architectural decisions prior to deployment.

National space agencies and defence missions often benefit from classified threat intelligence, geopolitical analyses, and upstream supply chain reporting that offer high-fidelity insights into adversary activity (Bradbury et al., 2020). Commercial NewSpace operators, by contrast, rely heavily on OSINT, commercial feeds or vendor-supplied advisories. This asymmetry is significant, as state actors often possess superior threat visibility compared to the organisations operating high-value orbital assets, particularly in communications, imaging, and IoT-integrated constellations (Maple et al., 2024).

CTI ingestion remains largely manual. Operators rarely automate CTI correlation with telemetry, configuration states, or detection rules. Ground segment SOCs often employ generic SIEM and EDR tools lacking satellite-specific context, leading to gaps in anomaly detection and mission-aware analysis (Varadharajan & Suri, 2022). As a result, CTI seldom informs detection engineering, attack-path evaluation or mission impact modelling, contributing to slow identification of ground side intrusions and incomplete visibility across segments.

Current CTI use is heavily concentrated on terrestrial infrastructure, malware alerts, credential-theft campaigns, and intrusion-set profiling reflecting where most adversary activity is detectable (Peled et al., 2023). However, CTI is infrequently applied to orbital-specific risks such as payload manipulation, inter-satellite link exploitation, onboard firmware anomalies, or telecommand authentication weaknesses. Literature consistently notes that the orbital domain remains underrepresented in intelligence-led planning (Willbold et al., 2023).

Space ISACs, cross-agency groups and vendor led forums have emerged to facilitate CTI exchange but participation is inconsistent and heavily influenced by cultural and legal constraints. Liability concerns, classification regimes and reputational risk reduce transparency particularly among commercial operators and international partners (Plotnek, J. J., & Slay, J. 2022; Vasquez, 2024). Consequently, shared intelligence often consists of high-level advisories rather than actionable indicators or behavioural insights.

A small number of operators are beginning to adopt more advanced CTI practices, including:

- Monitoring adversary interest in specific missions, sectors, or payload types
- Integrating CTI into supplier assurance and supply chain vetting
- Using CTI to forecast targeting likelihood during geopolitical escalation (Tedeschi, 2022)
- Incorporating CTI into pre-launch red team scenarios and validation exercises.

These practices remain exceptions but reflect early movement toward a more strategic use of intelligence.

Commercial NewSpace operators are disproportionately reliant on opensource and commercially available CTI, resulting in a broader but less curated threat picture. In contrast, traditional agencies benefit from high confidence classified intelligence but face integration and dissemination constraints. This divergence creates fundamentally different challenges in operationalising CTI for resilience.

Table 3: CTI Consumption Models. Traditional vs NewSpace

Dimension	Traditional Agencies	Commercial NewSpace
CTI Sources	Classified intel, government sharing	OSINT, commercial feeds, vendor intel
Timeliness	Often delayed but high fidelity	Near real time but variable quality
Integration	Structured, policy-driven	Ad hoc, tool driven
Security Posture	Risk-averse, compliance-heavy	Agile, speed to market focused
Automation	Limited due to classification constraints	Increasing but immature
Threat Coverage	Nation-state focused	Broader cybercrime, supply chain, opportunistic attackers

Overall, CTI use in space systems remains predominantly reactive, ground centric and reliant on manual workflows. Few operators leverage CTI to anticipate adversary behaviour, drive architectural decisions, or develop mission-specific detection logic. These limitations reinforce the sector's reactive posture and directly inform the barriers examined in the next section.

8. Barriers to CTI-Informed Resilience

Barriers to the systematic integration of Cyber Threat Intelligence (CTI) into space system security and resilience emerge across organisational, technical, and regulatory dimensions. These obstacles collectively contribute to the fragmented, reactive posture observed across the current space-cybersecurity landscape.

8.1 Organisational Barriers

Space missions traditionally separate disciplines into engineering, operations, mission assurance, and cybersecurity silos. This division creates misalignment around CTI ownership, interpretation, and operational use. In many organisations, no single role or team is responsible for translating intelligence into engineering or operational decisions, resulting in CTI being consumed passively rather than operationalised (Ahmad et al., 2023).

Moreover, CTI often competes with mission priorities such as launch schedules, payload performance, and cost efficiency. For commercial operators, time-to-market pressures and resource constraints further reduce incentives for integrating CTI into early design phases. The literature also highlights **workforce limitations**, particularly the shortage of personnel who understand both space mission architecture and intelligence-led cybersecurity (Kavallieratos & Katsikas, 2023). This skills gap makes it difficult to maintain continuous CTI analysis or embed intelligence into engineering reviews.

Trust barriers also play a role. Within multinational missions or consortia, partner organisations may hesitate to share sensitive intelligence due to reputational or liability risks, even when that intelligence would enhance collective resilience (Falco et al., 2024). This constrains situational awareness across the ecosystem.

8.2 Technical Barriers

Technical constraints significantly hinder the operationalisation of CTI across space systems. Most space operators rely on manual review of advisories and threat reports. Few possess systems that automatically correlate CTI with telemetry, system configurations, or known attack vectors. This limits the ability to rapidly detect emerging threats or adapt defences in real time (Borges Amaro et al., 2022).

Space systems typically incorporate diverse subsystems, proprietary protocols, and custom interfaces sourced from multiple vendors across long supply chains. This results in inconsistent security baselines and complicates the integration of standardised CTI-driven controls. As observed in recent experimental research, even satellites using widely adopted COTS components exhibit inconsistent firmware protections and update mechanisms (Willbold et al., 2023).

Onboard computing and power availability limit the deployment of advanced telemetry collection, real-time analytics, or autonomous CTI-driven defensive actions. Satellites also operate under strict bandwidth restrictions, meaning that CTI-relevant data (e.g., anomaly traces, system logs) may not be transmitted to the ground at the fidelity needed for threat analysis (Varadharajan & Suri, 2022).

Space architectures rely on dynamic, interdependent interactions between ground facilities, satellites, user terminals, cloud-based mission systems, and commercial communication networks. The absence of unified monitoring mechanisms prevents CTI-informed correlation across segments, making it difficult to detect attacks that traverse boundaries, such as ground-to-orbit exploitation or compromised user terminals influencing mission operations.

8.3 Regulatory and Policy Barriers

CTI integration also depends heavily on broader governance structures and legal frameworks. Several key issues arise.

Different jurisdictions vary in whether they classify space systems as critical infrastructure. Countries such as Australia and the UK recognise space as critical infrastructure, whereas the United States has historically avoided formal designation (Bradbury et al., 2020; Vasquez, 2024). These inconsistencies create mismatched obligations for reporting, incident disclosure, and CTI sharing.

International Traffic in Arms Regulations (ITAR), national security classifications, and commercial confidentiality all limit how much intelligence can be shared between partners. Such restrictions can prevent operators from accessing high-fidelity intelligence about threats that directly target their own systems (Jakhu & Pelton, 2017).

While initiatives such as IEEE P3349 and guidance from CISA aim to increase consistency, they remain voluntary or fragmented across agencies. Without mandatory CTI-sharing requirements or standardised exchange formats, intelligence dissemination remains informal and uneven (CISA, 2024).

Operators may hesitate to share detailed incident data because doing so could imply security deficiencies, trigger regulatory scrutiny, or expose them to contractual penalties. The absence of legal safe-harbour provisions for space-related CTI sharing exacerbates this reluctance.

Collectively, these barriers demonstrate that CTI integration depends as much on organisational culture and international governance as on technological capability. Overcoming them will require coordinated evolution in policy, engineering practices, information-sharing norms, and investment in mission-aware intelligence processes. The effectiveness of CTI-informed resilience is therefore contingent not only on better data, but also on the ecosystem's ability to translate that intelligence into consistent, shared and actionable security practice.

9. Discussion and Implications

The analysis demonstrates that effective CTI integration demands embedding intelligence as part of systems engineering rather than post-incident analysis. The implications extend beyond technology, requiring governance realignment, international trust frameworks, and sustained investment in CTI automation. Continuous CTI-fed resilience engineering can shift organisations from reactive patching to predictive defence.

Trade-offs emerge around autonomy, bandwidth, and data classification. Balancing these against resilience goals requires risk informed decision-making, and cross sector collaboration (Tedeschi, 2022). For policy makers, CTI integration highlights the urgency of harmonised standards and reciprocal disclosure agreements.

10. Conclusion and Proposed Research Agenda

This study examined two central questions: how CTI is currently used within space system security and what organisational, technical and regulatory barriers limit CTI-informed resilience. The analysis demonstrates that CTI adoption in the space sector remains fragmented and uneven, with most applications concentrated in terrestrial infrastructure and post disclosure vulnerability management. Intelligence rarely influences architectural decision making, interface assurance or mission specific detection logic, leaving a persistent gap between strategic awareness and operational practice.

Barriers across organisational structures, technical constraints and regulatory environments further limit the systematic integration of CTI. These obstacles reinforce a predominantly reactive security posture at a time when threat actors, geopolitical tensions and rapid commercial expansion are accelerating cyber risk across the space domain.

By synthesising trends across the existing literature, this paper establishes a foundation for understanding the role CTI should play in shaping resilient space systems. To support this transition, this paper introduces the **Operational Resilience through Behavioural Intelligence and Threat Integration (ORBIT)** framework as a conceptual workflow for operationalising CTI into adaptive, mission aware security processes.

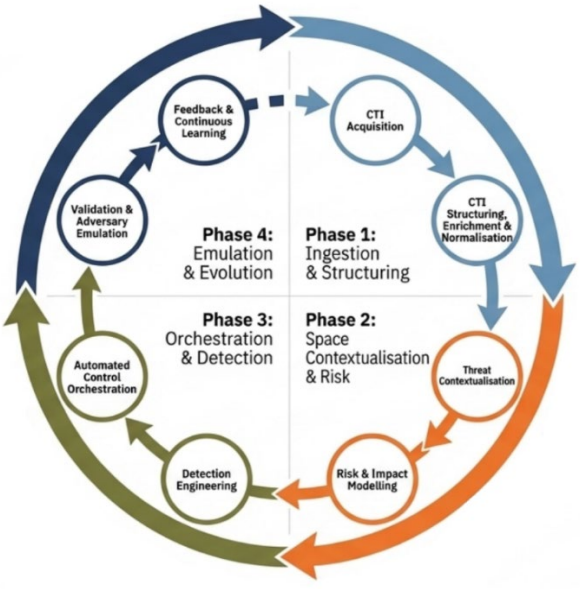

Figure 1: ORBIT Workflow Phases

Building on this foundation, addressing the identified gaps requires a structured research agenda focused on advancing the automated translation of CTI into detection and response controls, developing space specific threat modelling approaches that contextualise intelligence across ground, space and communication segments and extending existing frameworks to better reflect space system behaviours. Further research is needed to establish trust and validation mechanisms for automation in safety critical environments, enable effective integration of diverse intelligence sources and define measurable resilience metrics such as detection coverage and the latency between CTI ingestion and control deployment.

Taken together, these findings highlight the necessity of treating CTI not as an adjunct capability, but as a core architectural input to securing the space domain. Advancing this field will require a shift from reactive, manually

driven practices towards adaptive, intelligence-led resilience capable of evolving alongside both the threat landscape and the critical services that space systems underpin.

Ethics Declaration: Ethical clearance was not required for this research in accordance with institutional and national guidelines, as the study did not involve human or animal subjects, nor the collection of personal or sensitive data.

AI Declaration: AI assisted technologies were used only for proofreading and language refinement. They did not contribute to the conceptual development, methodological design, data analysis, or interpretation of results. The author retains full responsibility for the accuracy and integrity of the work.

References

Ahmad, A., Kotsias, J. and Scheepers, R. (2023) Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, 32(1), pp. 35–51.

Borges Amaro, L.J., Percilio Azevedo, B.W., Lopes de Mendonça, F.L., Albuquerque, R. de O. and García Villalba, L.J. (2022) Methodological framework to collect, process, analyse and visualise cyber threat intelligence data. *Applied Sciences*, 12(3), 1205. doi:10.3390/app12031205.

Boschetti, N., Gordon, N.G. and Falco, G. (2022) Space cybersecurity lessons learned from the ViaSat cyberattack. *Proceedings of the AIAA ASCEND Conference*, Paper AIAA 2022-4380. doi:10.2514/6.2022-4380.

Bradbury, M., Maple, C., Yuan, H., Atmaca, U.I. and Cannizzaro, S. (2020) Identifying attack surfaces in the evolving space industry using reference architectures. *Proceedings of the IEEE International Conference on Space System Security (SPACSEC)*, pp. 1–10.

Casaril, F. and Galletta, L. (2024) Securing SatCom user segment: a study on cybersecurity challenges in view of IRIS². *Computers & Security*, 140, 103799. doi:10.1016/j.cose.2024.103799.

Cyber and Infrastructure Security Centre (CISC) (2024) Positioning, Navigation and Timing (PNT) factsheet. Australian Government.

Cybersecurity and Infrastructure Security Agency (CISA) (2024) Recommendations to space system operators for improving cybersecurity. Washington, DC: U.S. Department of Homeland Security.

Ettinger, J. (2019) Cybersecurity of satellite ground station infrastructure. SANS Institute White Paper.

Falco, G. (2019) Cybersecurity principles for space systems. *Journal of Aerospace Information Systems*, 16(2), pp. 61–70.

Falco, G., Boschetti, N., Viswanathan, A., Gordon, N.G., Bodeau, D. and Salwen, J. (2024) Minimum requirements for space system cybersecurity: ensuring cyber access to space. *Proceedings of the IEEE International Conference on Space System Cybersecurity*, IEEE.

Falco, G., Boschetti, N., Viswanathan, A., Bailey, B., Maple, C., Kurt, G.K., Willbold, J., Slay, J., Birrane, E., Logsdon, D., Bennett, S., Ferguson, W., Curbo, J., Oakley, J., Schloegel, M., Hagen, S., Sigholm, J., Mehlman, C., Thummala, R., Calabrese, M., Shah, Y. and Le, A.T. (2024) Minimum requirements for space system cybersecurity – Ensuring cyber access to space. *Proceedings of the IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, Mountain View, CA, USA, pp. 78–88.

Hutchins, E.M., Cloppert, M.J. and Amin, R.M. (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Proceedings of the Lockheed Martin Cyber Security Symposium*, pp. 1–14.

Jakhu, R. and Pelton, J.N. (2017) *Global space governance: an international study*. Cham: Springer.

Kavallieratos, G. and Katsikas, S. (2023) An exploratory analysis of the last frontier: a systematic literature review of cybersecurity in space. *International Journal of Critical Infrastructure Protection*, 43, 100640.

Livingstone, D. and Lewis, P. (2016) *Space, the final frontier for cybersecurity?* Research Paper. London: Chatham House.

Maple, C., Bradbury, M., Yuan, H., Farrell, M., Dixon, C., Fisher, M. and Atmaca, U.I. (2020) Security-minded verification of space systems. In *Proceedings of the 2020 IEEE Aerospace Conference*, Big Sky, Montana, USA, 7–14 March 2020. IEEE.

Pavur, J. and Martinovic, I. (2022) Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity*, 8(1), tyac008.

Peled, R., Aizikovich, E., Habler, E., Elovici, Y. and Shabtai, A. (2023) Evaluating the security of satellite systems.

Saha, S.S., Rahman, S., Ahmed, M.U. and Aditya, S.K. (2019) Ensuring cybersecure telemetry and telecommand in small satellites: recent trends and empirical propositions. *IEEE Aerospace and Electronic Systems Magazine*, 34(8), pp. 34–49.

Slay, J., Uhongora, U., Plotnek, J., Law, Y.W. and Mulinde, R. (2023) Applying the SPARTA Matrix to develop intelligent security controls for space systems. *ASCEND 2023*.

Tedeschi, P., Sciancalepore, S. and Di Pietro, R. (2022) Satellite-based communications security: a survey of threats, solutions, and research challenges. *Computer Networks*, 216, 109246.

Varadharajan, V. and Suri, N. (2022) Security challenges when space merges with cyberspace. *arXiv*, abs/2207.10798.

Vasquez, C. (2024) Space is essential for infrastructure. Why isn't it considered critical? *CyberScoop*, 1 April.

Vollmer, B.K. (2021) NATO's mission-critical space capabilities under threat: cybersecurity gaps in the military space asset supply chain. *MA thesis*, Sciences Po Paris. arXiv:2102.09674.