© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722886

Cybersecurity Risks in Satellite Ground-Segment Infrastructure: Threat Profiling and Analysis

ANTHONY M. AKAGWU[1], ABDULRASHEED BADAMASUIY[2], CHINEDU CHIME[3], ALI M. MOHAMMED[4], ABBAS SALAMATU[5], AISHA YAKUBU[6], EJAH MOSES ODE[7], ISRAEL DICKSON[8]

[1, 2, 3, 4, 5, 6, 7, 8] *National Space Research and Development Agency (NASRDA)*

Abstract- ***Satellite systems are integral to telecommunications, navigation, Earth observation, defense, and other critical infrastructures. A satellite system comprises space, ground, and communication-link segments, with the ground segment providing command, control, telemetry, and data-processing functions. This paper examines cybersecurity risks within satellite ground-segment infrastructure through structured threat profiling and risk analysis.***

Despite growing attention to satellite security, existing literature often addresses space and ground segments together, making it difficult to isolate ground-specific threats, actors, and consequences. To address this gap, this study develops a threat-profiling framework based on six dimensions: threat actors, attack vectors, targeted assets, vulnerabilities, attack objectives, and potential impact. It maps major ground-segment assets including Mission Operations Centers, ground stations, TT&C systems, and cloud platforms, and analyzes how conventional cyberattacks can propagate into mission-critical environments. Using a qualitative risk model of Risk = Likelihood × Impact, the paper prioritizes threats and classifies them into Low, Moderate, High, and Critical levels. Credential compromise, malware/ransomware, and command/data manipulation are identified as critical risks due to high likelihood and potential to disrupt satellite operations. The study concludes that protecting ground-segment infrastructure requires a layered, defense-in-depth approach aligned with NIST cybersecurity principles, encompassing identity management, network segmentation, supply-chain controls, and incident response. The findings provide a threat-oriented foundation for developing more resilient cybersecurity measures for satellite ground operations.

Keywords: satellite ground segment, cybersecurity, threat profiling, risk assessment, critical infrastructure, command and control, space systems

I. INTRODUCTION

The increasing integration of space-based systems into telecommunications, navigation, Earth observation, defense, financial services, disaster management, and other critical activities has made satellite infrastructure an important component of modern digital ecosystems. Satellite systems are generally composed of interdependent space, ground, and communication-link segments, with the ground segment providing the infrastructure through which satellites are monitored, controlled, and supported. Consequently, the security of the ground segment is closely connected to the overall security and operational continuity of satellite missions ;.

The ground segment is particularly significant from a cybersecurity perspective because it connects space assets to terrestrial information and communication infrastructure. Mission operations centres, ground stations, telemetry, tracking and command (TT&C) systems, data-processing platforms, operator workstations, networks, and increasingly cloud-based services may form part of this environment. These interconnected components create multiple potential entry points for malicious actors. NIST's ground-segment cybersecurity framework emphasizes that the ground segment performs critical command-and-control functions and therefore requires mechanisms for identifying threats, protecting infrastructure, detecting compromise, responding to incidents, and recovering from operational disruptions .

The expansion of commercial and software-intensive space systems has further increased the complexity of this threat environment. Dependence on commercial off-the-shelf (COTS) technologies, third-party software, open-source components, cloud infrastructure, remote-access technologies, and

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722886

globally distributed supply chains can introduce vulnerabilities that extend beyond traditional ground-station security. Supply-chain exposure, legacy systems, weak configurations, human error, limited visibility, and increasingly sophisticated cyberattacks are among significant cybersecurity challenges affecting contemporary satellite systems .

Despite growing attention to satellite cybersecurity, much of the existing literature considers satellite security from a broad space-ground-link perspective. This can make it difficult to distinguish the specific threats, attack vectors, targeted assets, threat actors, and potential consequences associated with the ground segment. Recent research has demonstrated the breadth of cybersecurity challenges across satellite communications, while dedicated frameworks such as NISTIR 8401 provide a basis for applying cybersecurity risk management specifically to satellite ground operations ;.

This paper therefore focuses specifically on cybersecurity risks within satellite ground-segment infrastructure, with emphasis on threat profiling and analysis. It identifies major ground-segment assets and attack surfaces, profiles relevant threat actors and attack vectors, analyses major cybersecurity threats and their potential consequences, and proposes a structured approach for prioritizing these risks. The objective is to provide a concise threat-oriented perspective that can support the development of more resilient cybersecurity measures for satellite ground operations.

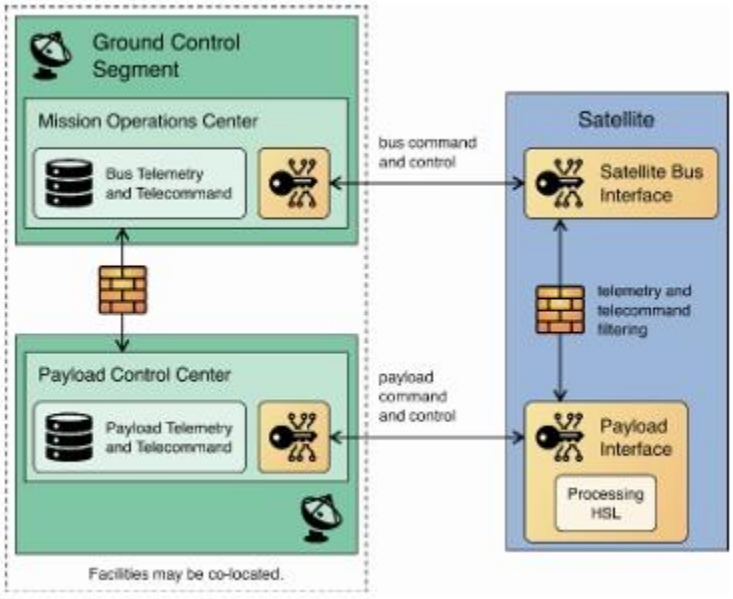

Figure 1. Satellite Ground-Segment Architecture .

II. SATELLITE GROUND-SEGMENT INFRASTRUCTURE AND ATTACK SURFACE

The satellite ground segment comprises the terrestrial facilities, systems, networks, and personnel responsible for communicating with, controlling, and supporting space assets. It forms the operational bridge between the spacecraft and terrestrial users and infrastructure. Within this environment, the Mission Operations Center (MOC) provides command and control of the satellite bus and receives telemetry, tracking, and command (TT&C) information, while the Payload Control Center (PCC) provides command and control functions for satellite payloads .

Components of the Ground Segment

A typical ground segment consists of several interconnected components. Ground stations provide the radio-frequency interface through which commands are transmitted to spacecraft and telemetry and mission data are received. Mission Operations Centers process operational information and execute

command-and-control activities, while Payload Control Centers manage mission-specific payload functions. These facilities are supported by communication networks, servers, data-processing systems, operator workstations, authentication systems, and increasingly cloud-based computing resources. NIST identifies systems, networks, and capabilities that interact with the satellite bus as part of the broader ground-segment environment (Lightman et al., 2023).

The increasing integration of conventional information-technology infrastructure with space operations has consequently expanded the ground segment beyond physically isolated control facilities. Cloud services, remote-access technologies, third-party platforms, and interconnected enterprise networks can provide operational efficiency but also introduce additional dependencies and potential points of compromise. Ground segment is a distinct asset category within commercial satellite systems and considers its interaction with other segments when assessing space-sector threats .

The attack surface represents the collection of physical, digital, human, and communication interfaces through which an adversary may attempt to compromise ground-segment assets. The extensive connectivity of the ground segment makes it particularly important from a cybersecurity perspective. Australia's Cyber Security Centre notes that ground systems are among the most interconnected elements of space systems because of their extensive connections to terrestrial networks, making them susceptible to threats such as malware, social engineering, denial-of-service attacks, compromised credentials, and software vulnerabilities .

Attack surfaces can therefore occur at several levels. At the physical level, remote ground facilities and equipment may be exposed to unauthorized physical access or tampering. At the network level, communication interfaces, gateways, virtual private networks, and other network connections may provide opportunities for intrusion or disruption. At the application level, vulnerabilities in mission-control software, APIs, operating systems, and cloud applications may be exploited. At the human level, operators and administrators may become targets of phishing, social engineering, credential theft, or insider activity. These attack pathways are particularly significant because compromise of a ground segment can potentially provide a pathway toward the systems responsible for controlling spacecraft. The European Space Agency's SPACE-SHIELD framework explicitly identifies ground-segment compromise as a potential stepping stone toward compromise of the space segment .

The diversity of these assets demonstrates that ground-segment cybersecurity cannot be reduced to protecting the antenna or ground station alone. Instead, security must encompass the entire ecosystem of physical infrastructure, command-and-control systems, networks, software, cloud resources, personnel, and external dependencies. This broader view is essential for the threat profiling undertaken in this scholarly work.

III. THREAT PROFILING FRAMEWORK FOR SATELLITE GROUND-SEGMENT SYSTEMS

Threat profiling provides a structured means of examining cybersecurity risks by connecting threat actors, attack vectors, targeted assets, vulnerabilities, objectives, and potential consequences. This approach is particularly appropriate for satellite ground-segment infrastructure because the ground environment comprises heterogeneous systems and personnel with different levels of exposure and operational importance. NIST's ground-segment cybersecurity profile emphasizes the identification and classification of systems, processes, and components as a basis for determining cybersecurity risk, while similarly adopts an asset- and threat-oriented taxonomy for analyzing satellite cybersecurity.

In this study, threat profiling is organized around six interconnected dimensions:

- threat actors,
- attack vectors,
- targeted assets,
- vulnerabilities,
- attack objectives, and
- potential impact.

The framework provides a common structure for comparing different threats before their relative risks are assessed.

Threat Actors

Threat actors represent the individuals, groups, or organizations capable of deliberately exploiting weaknesses within ground-segment infrastructure. Relevant actors include state-sponsored or nation-state groups, cybercriminals, hacktivists, malicious insiders, private-sector offensive actors, and other technically capable adversaries. identifies several of these categories within its space-sector threat assessment, reflecting the increasing diversity of actors that may target satellite infrastructure.

The motivation and capability of the actor influence the nature of the threat. For example, financially motivated attackers may priorities ransomware or credential theft, whereas state-linked actors may pursue espionage, disruption, or strategic access to satellite infrastructure. Consequently, threat profiling should consider not only the technical mechanism of an attack but also the likely capability and objective of its perpetrator .

Attack Vectors

Attack vectors describe the pathways through which an adversary can gain access to or interfere with ground-segment systems. These include phishing and social engineering, exploitation of software vulnerabilities, compromised credentials, malware, network intrusion, insecure remote access, API exploitation, supply-chain compromise, and physical access. The extensive integration of terrestrial IT infrastructure with satellite operations creates opportunities for conventional cyberattacks to propagate into mission-critical environments

This is significant because the ground segment does not operate as an isolated technical environment. Remote administration, interconnected networks, third-party services, and cloud-based infrastructure can increase operational flexibility while simultaneously expanding the number of possible attack pathways.

Assets and Vulnerabilities

Threat profiling must establish what is being targeted and why it is vulnerable. Ground stations, TT&C systems, mission-control centres, payload-control systems, operator workstations, network infrastructure, cloud platforms, and data repositories represent different assets with different security requirements. NISTIR 8401 specifically focuses on systems and capabilities supporting satellite command and control, recognizing that compromise of these systems can affect the management of space vehicles and payloads .

Vulnerabilities may arise from outdated software, insecure configurations, weak authentication, inadequate network segmentation, exposed interfaces, human error, legacy technologies, or weaknesses introduced through third-party components. identifies several of these factors within its assessment of commercial satellite cybersecurity.

The final dimensions concern what the attacker seeks to achieve and what consequences may result. Objectives may include unauthorized access, data theft, espionage, service disruption, command manipulation, sabotage, or system takeover. The resulting impact can be assessed against the confidentiality, integrity, and availability of ground-segment systems.

Of particular concern is the possibility that compromise of a terrestrial ground system may extend beyond the immediate IT environment and affect satellite operations. This makes threats involving command systems especially significant because an attack that compromises the integrity or authenticity of commands may potentially produce consequences in the space segment .

Table 1. Threat-Profiling Dimensions

Profiling dimension	Key question	Examples
Threat actor	Who may conduct the attack?	Nation-state, cybercriminal, insider, hacktivist
Attack vector	How can access or	Phishing, malware, vulnerability

	disruption occur?	exploitation, supply chain
Vulnerability	What weakness can be exploited?	Weak credentials, misconfiguration, unpatched software
Target asset	What ground component is targeted?	Ground station, TT&C, MOC, cloud, workstation
Attack objective	What does the attacker seek to achieve?	Espionage, disruption, data theft, command manipulation
Potential impact	What could result from successful exploitation?	Loss of confidentiality, integrity, availability, operational disruption
Risk level	How significant is the threat?	Low, Moderate, High, Critical

The framework therefore establishes a consistent basis for analyzing the threats discussed in this paper. Rather than treating cybersecurity threats as an undifferentiated list, it enables each threat to be examined according to who conducts it, how it is executed, what weakness it exploits, what asset it targets, what objective it serves, and what consequences may follow. This provides the analytical foundation for the threat assessment and prioritization undertaken later in the paper.

IV. RISK ASSESSMENT AND THREAT PRIORITIZATION

The identification of cybersecurity threats alone does not establish which threats require the greatest level of attention. Risk assessment is therefore necessary to determine the relative significance of the threats identified in the preceding section. In satellite ground-segment environments, risk is influenced by both the likelihood of successful exploitation and the consequences of compromise. NIST's Cybersecurity Framework provides a risk-management approach based on identifying, protecting, detecting, responding to, and recovering from cybersecurity events, while ENISA's space-sector assessments similarly associate threats with targeted assets, attack scenarios, and potential impacts .

For this study, threats are qualitatively prioritized using the relationship:

$$Risk = Likelihood \times Impact$$

Likelihood represents the estimated possibility that a threat can successfully exploit a ground-segment vulnerability, considering factors such as accessibility, attack complexity, and the availability of established attack techniques. While *Impact* represents the potential consequences of successful exploitation, including compromise of confidentiality, integrity, or availability and, where applicable, disruption of satellite operations.

Threat Risk Classification

The threats identified in this section consequently be classified into four broad levels: Low, Moderate, High, and Critical. The classification is intended as a comparative analytical assessment rather than a universal numerical risk score, since actual risk will vary according to the architecture, security controls, mission criticality, and threat environment of individual satellite operators.

Table 2: Risk Prioritization of Satellite Ground-Segment Cybersecurity Threats

Threat	Likelihood	Potential impact	Priority
Credential compromise	High	High	Critical
Command/data manipulation	Medium	Very High	Critical
Malware/ransomware	High	High	Critical

Threat	Likelihood	Potential impact	Priority
Network intrusion/DoS	High	Medium–High	High
Supply-chain compromise	Medium	Very High	High
Insider threat	Medium	High	High

The assessment indicates that credential compromise, malware, and command/data manipulation warrant particular attention. Credential compromise has a relatively high likelihood because human users and remotely accessible accounts provide potential entry points. Its impact can become critical where compromised credentials provide privileged access to mission-control systems. Malware similarly presents a high-priority threat because it can spread across interconnected ground infrastructure and disrupt mission-support functions.

Command and data manipulation presents a different risk profile. Its likelihood may be comparatively lower where strong authentication and command-validation mechanisms are implemented; however, the potential impact is considerably greater because unauthorized or manipulated commands could affect spacecraft operations. The combination of relatively lower probability and potentially severe consequences therefore justifies its critical classification .

Supply-chain compromise also deserves high priority because its effects may extend across multiple organizations and remain difficult to detect when malicious components or compromised software enter the environment through trusted suppliers. ; highlights supply-chain vulnerabilities, third-party dependencies, legacy systems, and human factors as important elements of the contemporary space cybersecurity risk landscape.

Risk Prioritization Implications

The analysis demonstrates that threat frequency should not be the sole basis for prioritization. A relatively infrequent attack can represent a critical risk when it targets a highly privileged or mission-critical component. Conversely, a frequent attack may have a lower operational consequence when effective segmentation and recovery mechanisms prevent it from reaching critical systems.

This distinction is particularly important for satellite ground segments because cybersecurity failures can have consequences beyond the terrestrial IT environment. Protecting administrative networks while leaving command-and-control pathways inadequately protected could allow an attacker to exploit the weakest link in the operational chain. Risk management should therefore prioritize assets according to mission criticality, access privileges, potential propagation pathways, and consequences of compromise .

The resulting prioritization also supports a defense-in-depth approach in which identity security, network segmentation, endpoint protection, supply-chain controls, continuous monitoring, and command authentication are implemented as complementary safeguards rather than isolated controls. This aligns with NIST's risk-management approach, which treats cybersecurity as a continuous process rather than a one-time technical intervention .

V. EMERGING GROUND-SEGMENT CYBERSECURITY RISKS

The cybersecurity environment of satellite ground segments is evolving as space operations increasingly incorporate commercial technologies, cloud computing, software-defined systems, automation, and interconnected terrestrial networks. These developments improve scalability and operational efficiency, but they also introduce additional dependencies and attack surfaces. identifies software-defined satellites, commercial off-the-shelf (COTS) and open-source components, supply-chain dependencies, and emerging technologies as factors contributing to the changing cyber-risk landscape of commercial satellite systems.

Cloud-Based Ground Infrastructure

Cloud computing is increasingly being incorporated into ground-segment operations, including data processing, storage, mission support, and Ground

Station as a Service (GSaaS). While cloud adoption can improve scalability and reduce infrastructure costs, it introduces risks associated with misconfiguration, identity and access management, exposed interfaces, multi-tenancy, and dependence on third-party providers. The UK's Department for Science, Innovation and Technology specifically identifies expanded attack surfaces and configuration weaknesses as important cybersecurity considerations for cloud-enabled ground segments ; .

Software-Defined and Automated Operations

The increasing use of software-defined technologies and automation can reduce manual intervention in satellite operations but may also increase the consequences of software compromise. Vulnerabilities in applications, APIs, automated workflows, or update mechanisms could potentially provide attackers with pathways into operational environments. consequently, identifies software-defined architectures and emerging technologies as developments requiring increased cybersecurity attention.

Artificial Intelligence and Advanced Cyber Threats

Artificial intelligence presents a dual challenge. It can strengthen threat detection and anomaly identification, but adversaries can also employ AI to improve phishing, social engineering, reconnaissance, malware development, and other malicious activities. Cybersecurity threat assessment in ground stations architecture identifies the abuse of AI as an emerging cybersecurity trend, suggesting that ground-segment operators will increasingly need to account for AI-enhanced attack techniques .

VI. CONCLUSION

The threat analysis indicates that protecting satellite ground-segment infrastructure requires a layered approach addressing identity, network security, command integrity, supply-chain exposure, and incident response. Rather than relying on a single security control, operators should combine preventive, detective, and recovery measures based on the criticality of individual ground-segment assets. This approach is consistent with the risk-management principles of the NIST Cybersecurity Framework and the ground-segment security guidance developed specifically for satellite command and control.

Strong identity and access management implemented across mission-critical systems ensures security of satellite ground assets using multi-factor authentication, least-privilege access, privileged-account management, and regular credential reviews measures which can significantly reduce the likelihood of credential compromise. Administrative access to mission control, TT&C and other critical systems should be restricted to authorized personnel and separated from ordinary enterprise accounts. Particular attention should be given to remote access because compromised credentials can provide attackers with a direct pathway into sensitive ground infrastructure.

Mission-critical components such as TT&C systems, mission-control networks and spacecraft interfaces should be logically isolated from less trusted enterprise and external networks. Firewalls, intrusion detection and prevention systems, security information and event management (SIEM), and network monitoring can improve the detection of anomalous activity.

REFERENCES

[1] Agrafiotis, I., Jason, N. R., Goldsmith, M., Creese, S., & pton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate . *Journal of Cybersecurit*.

[2] Angyalos-Porkoláb, Z., & Szilágyi , R. (2025). Cybersecurity Risks in Critical Infrastructures: Insights from CISA and ENISA Data . *Journal of Agricultural Informatics*.

[3] Bradbury, M., Maple, C., Yuan, H., Atmaca, U. I., & Cannizzero, S. (2020). Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures. *2020 IEEE Aerospace Conference*.

[4] Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection*.

[5] Casaril, F. (2026). Space Cyber Risk: A Hybrid Analysis of Threats, Policies, and Governance.

[6] Choi, H., Kwon, Y. E., & Yoon, J. W. (2026). Security assessment of Internet-exposed satellite ground segments via non-intrusive reconnaissance. *JOURNAL OF SPACE SECURITY*, 43-51.

[7] Deierlein, G. G., McKenna, F., Zsarnóczay, A., Kijewski-Correa, T., Kareem, A., Elhaddad, W., . . . Govindjee, S. (2020). A Cloud-Enabled Application Framework for Simulating Regional-Scale Impacts of Natural Hazards on the Built Environment. *Frontiers in Built Environment*.

[8] Hamill-Stewart, J., & Rashid, A. (2024). Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks. *Proceedings of the 2024 Workshop on Security of Space and Satellite Systems*, 1-5.

[9] Khan, M. S., Khan, M. A., Zia, M., Lais, M., & Khan, M. S. (2026). From GENSO to Next-Generation Collaborative CubeSat Operations Networks: A Framework for Distributed, AI-Enabled Satellite Missions in Emerging Space Nations. *Journal of Applied Technology Research and Innovation (JATRI)*.

[10] Kovvuri, A. C. (2026). How Vulnerable is the Space Segment? A Deep Dive into RF Links, Ground Controls, and Satellites. *Cybersecurity, Privacy, & Networks*.

[11] Lightman, S., Suloway, T., & Brule, J. (2022). *Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control* . NIST Interagency Report .

[12] Mohammed, A. (2023). Protecting Space Assets: Cybersecurity Challenges and Solutions for the Final Frontier. *Baltic Journal of Engineering and Technology*, 55-61.

[13] Nejad, B. (2022). Cyber Security. *ntroduction to Satellite Ground Segment Systems Engineering* , 223–244.

[14] Salim, S., Moustafa, N., & Reisslein, M. (2025). Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *IEEE Communications Surveys & Tutorials*, 372 - 425.

[15] Vanlyssel, J., Sobrados, E., Anwar, R., Roman, G.-C., & Anwar, A. (2025). SpyChain: Multi-Vector Supply Chain Attacks on Small Satellite Systems. *Cryptography and Security*.

[16] Verma, A. R. (2025). Cybersecurity in Satellite Communication Networks: Key Threats and Neutralization Measures. *IEEE Open Journal of the Communications Society*, 5667 - 5692.