© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722480

A Review of Emerging Cybersecurity Threats and Challenges in Satellite Communication Systems

IBRAHIM MUSTAPHA[1], LAURA YUSUF-UFUA[2], USMAN SALISU ARGUNGU[3]
[1,2,3]*National Space Research and Development Agency (NASRDA)*

Abstract- ***Satellite technology has evolved in modern development and deployment of various payloads to rely on the integration of existing terrestrial communication architecture. An almost secured industry to the use of proprietary off-the shelf software and onboard systems is now exposed to cyber threats that terrestrial communication network architectures struggle to deal with. This paper carried a holistic review of literatures that have investigated the causalities of cyber threats in cyber space in modern satellite systems. The general consensus identified by the literatures investigated attributed these challenges to the integration of space technology with traditional terrestrial communication networks. This has led to the inheritance of cyber challenges associated with terrestrial communication networks. The paper further identified some cyber threats that are presently affecting space communication architecture. Amongst others are, network spoofing, traffic jamming, Distributed Denial of Service (DDoS), API exploitation, Eavesdropping etc. Furthermore, the paper examined potential emerging threats to satellite communication architectures such as AI prompts to investigate and exploit vulnerabilities. The paper concluded by proposing emerging solutions to space communication architecture.***

Keywords: cybersecurity, threat landscape, and satellite communication systems

I. INTRODUCTION

The evolution of satellite communication systems has significantly transformed the global communications landscape, enabling ubiquitous connectivity for applications ranging from television broadcasting, disaster monitoring, global navigation, remote sensing, and broadband Internet access. The evolutionary history of satellite communication infrastructure is largely dominated by nation states and related agencies; and a significantly limited number of commercial operators utilizing geostationary Earth orbit (GEO) satellites. However, the emergence of the new space era, is heavily characterized by commercial space ventures, reusable launch vehicles, low-cost satellite manufacturing, software-defined payloads, and large Low Earth Orbit (LEO) constellations, has fundamentally reshaped the architecture, scope, capabilities and operation of satellite communication systems (Song, Gnyawali, & Qian, 2024) (Parkinson, 1997).

Global communications ecosystem, broadband connectivity, navigation, remote sensing, disaster response, military operations, and the operation of critical infrastructures have over the years come to rely on satellite communication systems as an indispensable component in their operations. Satellite communication systems have wide coverage area which is a limitation of terrestrial communication architecture. This feature makes satellite communication ideal for serving remote, maritime, and underserved regions where conventional communication infrastructures are either unavailable or economically impractical (Chen, Sun, & Kang, 2022) (Zhu & Jiang, 2022). Integration of satellite communication into fifth-generation (5G) and emerging sixth-generation (6G) non-terrestrial networks (NTNs) will further expand and support ubiquitous role of connectivity and global digital transformation (Chen, Sun, & Kang, 2022).

Over the past decade, the satellite industry has witnessed a profound shift which has expanded the number of constellations of LEO satellites in orbit, payloads and industry players to include significant input from the private sector that has seen a growing pool of services being commercialized. Advances such as software-defined satellites, onboard processing, cloud-integrated ground segments, and inter-satellite optical links have significantly enhanced the flexibility, scalability, and performance of satellite communication systems while enabling

new applications across commercial, scientific, and defense (Kodheli, et al., 2021).

While these technological advancements have accelerated the growth of space-based communications and associated systems, they have also fundamentally altered the cybersecurity landscape. Modern satellite communication systems are no longer isolated infrastructures but highly interconnected cyber-physical systems comprising satellites, terrestrial control stations, user terminals, cloud platforms, communication links, software-defined network components, onboard advanced computing chips and mission specific payloads built on modern day computing resources. This convergence with terrestrial information and communication technologies has substantially expanded the cyberattack footprint, exposing satellite infrastructures to increasingly sophisticated and persistent cyber threats (Mohammed, 2023) (Salim, Moustafa, & Reisslein, 2025) (Manulis, Bridges, Harrison, Sekar, & Davis, 2021).

Historically, cybersecurity was not considered during satellite mission design because many missions operated in relatively closed environments, relied on proprietary technologies, and communication hardware from the design, deployment and operations have enforced strict physical access protocol to development laboratories, mission control rooms and ground segment hardware installation. However, the increasing commercialization of space services, adoption of commercial off-the-shelf hardware, extensive software integration, and reliance on internet-connected ground infrastructures have exposed satellite development environments to challenges akin to terrestrial communication architecture. Consequently, satellite communication systems have become attractive targets for malicious cyber actors seeking to disrupt communications, compromise sensitive information, manipulate satellite operations, or degrade national critical infrastructure (Willbold, Sciberras, Strohmeier, & Lenders, 2024).

Cyber threats targeting satellite communication systems span multiple architectural layers and operational domains due to the vast footprint and likelihood of discovering vulnerabilities. Attacks such as jamming, spoofing, signal interception, and eavesdropping exploit the broadcast nature of wireless satellite transmissions which is mostly targeted at the communications layer. Network-layers are susceptible to routing protocols, inter-satellite links, or cloud-based management platforms attacks, while attacks on application-layer are increasingly focused on software vulnerabilities within mission control systems, virtualization platforms, and satellite payload software. Another attack surface is the supply chain compromises, insider threats, ransomware campaigns targeting ground stations, and malware infiltration which have further demonstrated that cybersecurity challenges are well beyond space segment (Rocionero-Garcia & Skaikh, 2024) (Wang, et al., 2026).

The evolution towards mega-constellations has opened a vast pool of threat landscape to be exploited by malicious adversaries. Unlike traditional satellite architectures, constellation-based systems require continuous coordination among satellites, automated resource allocation, dynamic routing, and extensive software orchestration. These characteristics increase system complexity while creating new opportunities for adversaries to exploit vulnerabilities across distributed satellite networks. Emerging technologies, including artificial intelligence (AI), machine learning (ML), software-defined networking (SDN), network function virtualization (NFV), and cloud-native satellite operations, simultaneously provide enhanced operational capabilities and introduce a host of cybersecurity risks that require adaptive, responsive and intelligent defense approaches (Verma, 2025) (Pavur & Martinovic, 2022) (Lin, Henry, & Dill, 2022).

This paper investigates various cyber threats, vulnerabilities and attack vectors that threatens the operations and functionality of satellite communication systems. The paper further identifies defense mechanisms to mitigate against the effect of cyber-attacks in the era of emerging space capabilities.

II. CYBERSECURITY LANDSCAPE OF SATELLITE COMMUNICATION SYSTEMS

The space sector has seen a major impact as to the effect of cyber threats to its operations and systems. Attacks that were initially thought as impossible are now critical issues to satellite resources. This shift is largely motivated by the value of data these systems transmit and process. Unlike traditional satellite infrastructures, which were primarily characterized by isolated architectures and limited external connectivity, contemporary satellite communication systems are highly interconnected, software-driven, and increasingly integrated with terrestrial communication networks. This transformation, driven by the new space paradigm, has significantly enhanced operational capabilities while simultaneously expanding the attack surface available to malicious actors both state and non-state (Carlo & Obergfaell, 2024).

2.1 Evolution of Satellite Communication Architectures

Conventional satellite communication systems were predominantly developed and deployed based on geostationary earth orbit (GEO) satellites designed for long operational lifespans and dedicated missions such as television broadcasting, weather monitoring, and military communications. These systems typically relied on proprietary hardware, centralized ground control, and relatively static communication architectures, which inherently limited external exposure to cyber threats. Although vulnerabilities existed, the isolationist designs of these systems and restricted access to operational networks reduces the likelihood of sophisticated cyber intrusions (Lamy, Le Fevre, & Sarli, 2012) (Wang, Luo, & Wu, 2020).

The new space ecosystem ushered in an alternate paradigm which has accommodated commercial enterprises that have now deployed large-scale constellations of low Earth orbit (LEO) satellites capable of providing global broadband connectivity with significantly lower latency than traditional GEO systems. Companies such as SpaceX's Starlink, OneWeb, and Amazon's Project Kuiper are at the forefront of this shift toward distributed satellite architectures designed to support high-speed internet access, Internet of Things (IoT) services, autonomous transportation, and future non-terrestrial network (NTN) applications (Geraci, López-Pérez, Benzaghta, & Chatzinotas, 2023) (Giordani & Zorzi, 2021).

Unlike conventional networks, modern satellite constellations operate as distributed networks composed of hundreds or even thousands of interconnected satellites in orbit. Communication increasingly occurs not only between satellites and ground stations but also through inter-satellite links (ISLs), enabling autonomous routing and data exchange across satellites in the constellation. This distributed architecture improves resilience and communication efficiency but also introduces additional network complexity and multiple points of vulnerability to be exploited (Jiang, et al., 2023).
Furthermore, satellite communication systems are becoming more integrated with 5G and emerging 6G terrestrial ecosystems. This convergence also exposes satellite networks to cybersecurity threats that have traditionally targeted terrestrial communication systems, including protocol exploitation, cloud-based attacks, and software vulnerabilities (Jiang, et al., 2023).

2.2 Modern Satellite Systems Security Requirements

The technological innovations defining the news space architectures have introduced several characteristics that significantly influence cybersecurity requirements.

A prominent feature is the widespread adoption of software-defined satellites (SDSs). Unlike conventional satellites with fixed onboard hardware functionalities, SDSs enable dynamic reconfiguration of communication payloads and network operations through software updates. While this flexibility improves functionality and enhanced capabilities, it exposes software to cyber-attacks via software manipulation. Unauthorized access to software management systems or compromised firmware updates could potentially affect multiple satellite functions simultaneously, making secure software lifecycle management a critical cybersecurity concern (Xu, Wang, & Huang, 2018).

Virtualized and cloud-based ground infrastructures solutions are now utilized by modern satellite operators frequently. These solutions employ cloud computing platforms for mission planning, telemetry processing, network management, and data analytics. Virtualization technologies and Software-Defined Networking (SDN) enable flexible resource allocation and scalable service delivery but these solutions inherit cybersecurity risks associated with cloud deployment environments, including misconfigurations, unauthorized access, insecure application programming interfaces (APIs), and supply chain vulnerabilities (Yuan, Peng, & Sun, 2025) (Kosmidis, Trompouki, Solé, Suárez, & Wolf, 2024).

Optical and radio-frequency inter-satellite links facilitate autonomous routing, cooperative resource management, and reduced dependence on ground segment infrastructure. Although these capabilities improve operational resilience and network efficiency, they also create opportunities for lateral cyberattacks, where the compromise of a single satellite or communication node may propagate across interconnected network segments appropriate network segmentation is not deployed and authentication mechanisms are weak or absent (Choudhary & Agrawal, 2024)

The application of Artificial Intelligence (AI) and Machine Learning (ML) are also increasingly integrated into satellite operations to optimize resource allocation, fault detection, spectrum management and autonomous decision-making especially on collision avoidance and telemetry guidance. These technologies improve operational efficiency but introduce new attack vectors, including adversarial machine learning, model poisoning, and data manipulation attacks that may compromise automated decision-making processes (Furano, Tavoularis, & Rovatti, 2020).

2.3 Cybersecurity Implications

The convergence of these technologies, software-defined architectures, cloud-native infrastructures, AI-enabled operations, ML, terrestrial communication architecture and large-scale satellite constellations has transformed satellite communication systems into complex cyber-physical ecosystems. Traditional solutions to existing satellite architecture have proven inadequate in addressing cybersecurity concerns solely through perimeter defenses or isolated communication encryption. Instead, security must consider the entire operational lifecycle, including satellite design, software development, launch operations, ground infrastructure, communication protocols, supply chain management, and system maintenance (Geraci, López-Pérez, Benzaghta, & Chatzinotas, 2023).

The interconnected nature of modern satellite networks means that vulnerabilities originating in terrestrial infrastructure may spill into space assets and vice versa. These architectural and operational convergence of satellite technology and terrestrial communication architecture establish the foundation for understanding the diverse cybersecurity challenges and sophisticated threat landscape satellite communication systems are exposed to.

III. EMERGING THREATS AND CYBERSECURITY CHALLENGES

The transition to the New Space paradigm has fundamentally reshaped the cybersecurity landscape of satellite communication systems. Unlike traditional satellite infrastructures, which were characterized by relatively isolated architectures and limited network connectivity, modern satellite systems operate as highly distributed, software-driven ecosystems integrating space, ground, cloud, and terrestrial communication networks. While these technological advancements have improved flexibility, scalability, and global connectivity, they have inadvertently expanded the attack surface, exposing satellite communication systems to increasingly sophisticated cyber threats (Peled, Aizikovich, Habler, Elovici, & Shabtai, 2023).

3.1 Infrastructure Vulnerabilities

Modern satellite networks comprise multiple interconnected components, including satellites, ground stations, mission control centers, user terminals, cloud platforms, and communication gateways. The security of all systems depends on the

resilience of individual component, as a breach in one segment can affect part or the entirety of the system.

Ground infrastructure remains one of the most vulnerable components of satellite communication systems due to human contact to physical systems. Mission control centers are responsible for telemetry, tracking, command (TT&C), software and firmware updates, and operational management. Because these facilities increasingly rely on internet-connected enterprise networks and cloud-based services, they inherit many of the cyber risks commonly associated with conventional communication infrastructures, including phishing attacks, ransomware, insider threats, credential theft, and remote exploitation (Boschetti, Gordon, & Falco, 2022). Recent cybersecurity assessments conducted indicate that attackers often target ground infrastructure rather than satellites themselves because terrestrial systems are more accessible and frequently contain legacy software or misconfigured security controls (Radack, 2003).

Security vulnerabilities with the supply chain of procurable with the space sector has also emerged as a critical security concern. The rapid commercialization of space has encouraged widespread adoption of commercial off-the-shelf (COTS) hardware and open-source software to reduce development costs and time of deployment. Although these technologies provide economic advantages, they may introduce vulnerabilities through compromised firmware, malicious software dependencies, counterfeit components, or violation of standards and practices. Consequently, cybersecurity must extend beyond operational environments to include the entire satellite development and deployment lifecycle (Kodheli, et al., 2021).

3.2 Communication Security Threats

Satellite communication links are inherently susceptible to attacks because wireless transmissions can be intercepted, disrupted, or manipulated without requiring physical access to space assets. Some of the most prevalent threats are;

i. Radio frequency (RF) jamming, where an adversary intentionally transmits interfering signals to degrade or completely deny communication services. Jamming attacks have been observed during military conflicts and represent a persistent threat to both civilian and defense satellite operations because they can disrupt navigation, broadcasting, and emergency communication services (Khan, et al., 2024)
ii. Signal spoofing attack in which malicious actors transmit manipulated signals that imitate legitimate satellite transmissions. Successful spoofing attacks can mislead receivers into accepting false positioning, navigation, or timing information, potentially affecting aviation, maritime navigation, autonomous vehicles, and critical infrastructure synchronization (Mohammed, 2024). As satellite systems increasingly support safety-critical applications, protecting signal authenticity has become a major research priority.
iii. Eavesdropping and signal interception remain persistent concerns due to the broadcast nature of satellite communications. Although modern encryption techniques have partly improved confidentiality, insecure key management, outdated cryptographic algorithms, improperly configured communication protocols, or emerging threats still evade these measures put in place (Yahia, Erdogan, Kurt, Altunbas, & Yanikomeroglu, 2022).

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722480

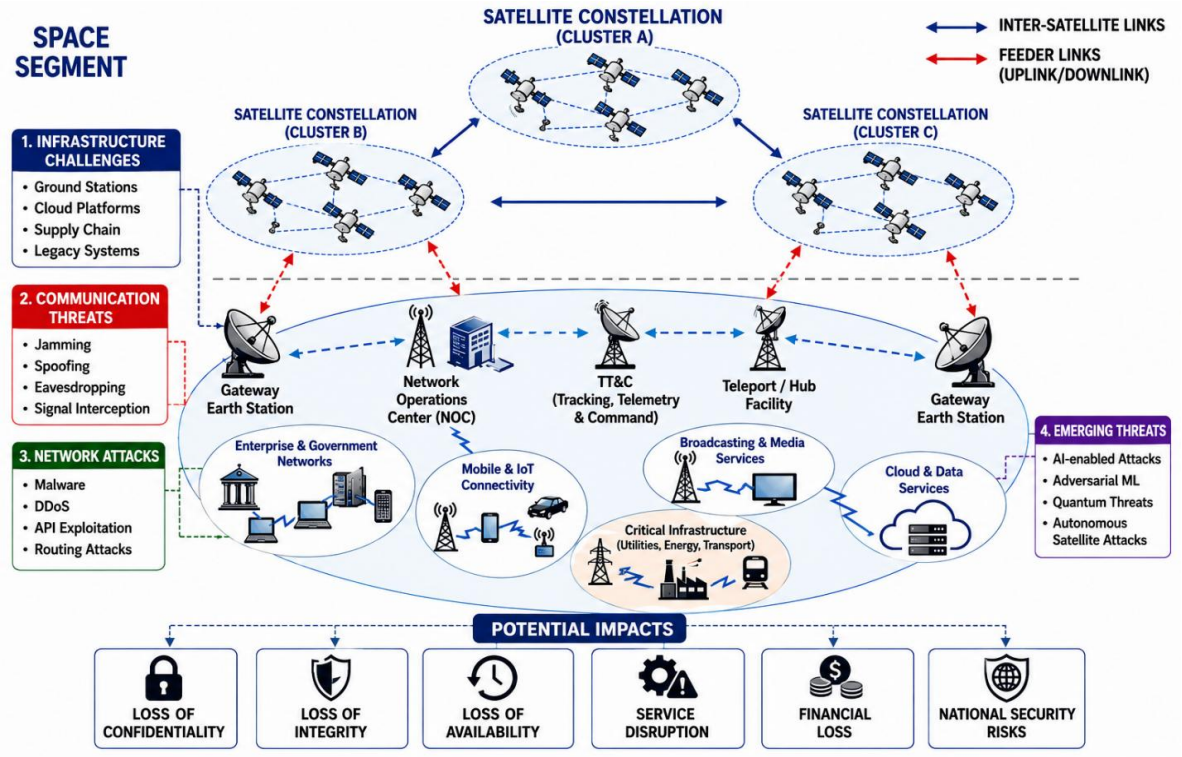

Figure 1: Taxonomy of Cybersecurity Challenges and Emerging Threats

3.3 Network and System-Level Attacks

The increasing software dependence of satellite communication systems has introduced numerous vulnerabilities that are traditionally associated with terrestrial communication networks. Software-defined satellites, virtualized ground infrastructures, cloud-based mission management platforms, and communication payloads all rely heavily on the integrity of the software it runs on. Consequently, an attack targeting software vulnerabilities through malware deployment, remote code execution, privilege escalation, and exploitation of insecure application programming interfaces (APIs) will certainly mean the compromise of the entire system in the communication architecture (Chiejina, Kim, Chowhdury, & Shah, 2024).

Distributed denial-of-service (DDoS) attacks represent another growing concern, particularly against ground stations and cloud-supported satellite solutions. Attackers can significantly degrade service availability, affecting satellite-based internet connectivity and mission operations by overwhelming critical assets that allow the processing of legitimate queries. As satellite operators increasingly integrate terrestrial cloud infrastructures into operational workflows, the likelihood of DDoS attacks affecting satellite services continues to increase (Giuliari, Ciussani, Perrig, & Singla, 2021).

3.4 Emerging Threats in the New Space Era

The rapid digitalization of satellite communication systems has introduced a new generation of cyber threats that extend beyond conventional attack techniques. Artificial intelligence (AI) has become a particularly significant concern because it can be leveraged by both defenders and adversaries. Attackers increasingly employ AI to automate vulnerability discovery, generate sophisticated phishing campaigns, evade intrusion detection systems, and optimize malware behavior. At the same time, AI-based satellite operations introduce vulnerabilities such as adversarial machine learning, model poisoning, and data manipulation attacks capable of compromising autonomous decision-making processes (Manulis, Bridges, Harrison, Sekar, & Davis, 2021).

Quantum computing is another potential emerging technology that presents another long-term cybersecurity challenge. Public-key cryptographic algorithms widely used for authentication and secure key exchange may become vulnerable to quantum attacks, potentially compromising secure communications between satellites, ground stations, and users. Although practical quantum attacks remain largely theoretical, researchers have increasingly advocated for the gradual adoption of post-quantum cryptographic algorithms to ensure the long-term security of satellite communication systems (Kendzierskyj, Jahankhani, & Hussien, 2024).

Another emerging concern involves the growing autonomy of satellite constellations. Future satellite networks are expected to incorporate autonomous navigation, dynamic resource allocation, self-repair capabilities, and distributed decision-making with minimal human intervention. While autonomy improves operational efficiency and resilience, it also introduces new cybersecurity risks because compromised autonomous functions may rapidly propagate erroneous decisions throughout an entire constellation. Ensuring trustworthy autonomous operations therefore represents a critical challenge for next-generation satellite communication systems (Araguz, Bou-Balust, & Alarcón, 2018)

Overall, the literature demonstrates that cybersecurity threats in the modern space era are becoming increasingly multidimensional, targeting communication channels, software platforms, network infrastructures, supply chains, and autonomous operational capabilities simultaneously. These evolving threats highlight the limitations of traditional perimeter-based security models and underscore the need for adaptive, layered, and intelligence-driven defense mechanisms. Accordingly, the next section examines the principal defense strategies proposed to enhance the cyber resilience of modern satellite communication systems.

IV. FUTURE RESEARCH DIRECTIONS

Future research should focus on developing comprehensive cybersecurity frameworks that address the unique characteristics of modern satellite communication systems. Several promising directions can be identified.

a. Future researches should investigate adaptive and autonomous cyber defense mechanisms that could be capable of detecting and responding to threats with minimal human intervention. Combining AI-based anomaly detection with secure autonomous response mechanisms to improve resilience against rapidly evolving attacks.
b. Employing Zero Trust architectures for space systems. Traditional security models based on network boundaries are increasingly ineffective in distributed satellite environments. Future satellite networks should adopt continuous authentication, dynamic authorization, and micro-segmentation principles to minimize the impact of compromised components. This principle ensures that nodes on the network must always authenticate at every session initiation.
c. Also, future researches should explore secure-by-design satellite development methodologies that incorporate cybersecurity from the earliest stages of system engineering. This includes secure software development practices, hardware assurance, supply chain protection, and automated vulnerability assessment throughout the satellite lifecycle.
d. Future studies must also examine cybersecurity solutions for integrated space-air-ground networks supporting 6G communications. As satellite systems become increasingly embedded within global communication infrastructures, security frameworks must address cross-domain risks involving satellites, terrestrial networks, Unmanned Aerial Vehicle (UAV) systems, and edge computing platforms.
e. Finally, stronger collaboration between governments, commercial satellite operators, cybersecurity researchers, and international standards organizations is required to establish common security practices for the rapidly expanding space economy. Since cyber threats against satellite systems often transcend national boundaries, effective protection will require coordinated approaches involving technical

innovation, regulatory frameworks, and information sharing mechanisms.

V. CONCLUSION

The rapid evolution of satellite communication systems within the modern space era has transformed space-based connectivity from a specialized capability into a critical component of the global digital infrastructure. The emergence of commercial satellite constellations, software-defined satellites, cloud-integrated ground systems, and non-terrestrial networks has significantly enhanced the scalability, flexibility, and accessibility of satellite services. However, these advancements have also introduced a complex cybersecurity environment characterized by expanded attack surfaces, increased system interconnectivity, and greater dependence on software-driven operations.

This paper explored literatures that investigates cybersecurity challenges in modern satellite communication systems at every level of mission development and deployment to extend across multiple architectural domains, including space assets, ground infrastructures, communication links, software platforms, supply chains, and user networks. Traditional threats such as jamming, spoofing, and eavesdropping remain persistent concerns, while emerging threats involving artificial intelligence-enabled attacks, software exploitation, autonomous satellite operations, and quantum computing present new challenges for future satellite security. The transition toward large-scale LEO constellations further amplifies these risks by introducing distributed architectures, dynamic network configurations, and complex operational dependencies.

The analysis of existing defense strategies demonstrates that securing future satellite communication systems requires a comprehensive, multi-layered approach rather than reliance on individual security mechanisms. Cryptographic protection, secure authentication, artificial intelligence-based threat detection, Zero Trust architectures, software-defined security mechanisms, and lifecycle-oriented security practices represent key components of a resilient satellite cybersecurity framework. However, significant challenges remain, particularly regarding the scalability of security solutions for mega-constellations, standardization of cybersecurity practices, validation of proposed mechanisms in realistic operational environments, and preparation for future quantum-enabled threats.

As satellite communication systems become increasingly integrated with terrestrial networks and future 6G infrastructures, cybersecurity must be considered a fundamental design requirement throughout the entire system lifecycle. Future research should prioritize adaptive, autonomous, and intelligence-driven defense mechanisms capable of responding to dynamic cyber threats while maintaining operational reliability. Additionally, stronger collaboration among researchers, commercial operators, government agencies, and international standards organizations will be essential for establishing effective cybersecurity governance within the expanding space ecosystem.

Ultimately, the security of modern satellite communication systems will depend on achieving a balance between technological innovation and cybersecurity resilience. By considering security-by-design principles, advanced defense technologies, and internationally coordinated security frameworks, future satellite networks can continue to provide reliable and secure communication services while supporting the growing demands of a connected global society.

REFERENCES

[1] Araguz, C., Bou-Balust, E., & Alarcón, E. (2018). Applying autonomy to distributed satellite systems: Trends, challenges, and future prospects. Systems Engineering, 401-416.

[2] Boschetti, N., Gordon, N. G., & Falco, G. (2022). Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. ASCEND.

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

[4] Chen, S., Sun, S., & Kang, S. (2022). System integration of terrestrial mobile communication and satellite communication —the trends, challenges and key technologies in B5G and 6G. IEEE 22nd International Conference on Communication Technology (ICCT).

[5] Chiejina, A., Kim, B., Chowhdury, K., & Shah, V. K. (2024). System-level Analysis of Adversarial Attacks and Defenses on Intelligence in O-RAN based Cellular Networks. Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 237-247.

[6] Choudhary, A., & Agrawal, N. K. (2024). Inter-satellite optical wireless communication (IsOWC) systems challenges and applications: a comprehensive review. Journal of Optical Communications, 925-935.

[7] Furano, G., Tavoularis, A., & Rovatti, M. (2020). AI in space: applications examples and challenges. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT).

[8] Geraci, G., López-Pérez, D., Benzaghta, M., & Chatzinotas, S. (2023). Integrating Terrestrial and Non-Terrestrial Networks: 3D Opportunities and Challenges. IEEE Communications Magazine, 42-48.

[9] Giordani, M., & Zorzi, M. (2021). Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities. IEEE Networks, 244-251.

[10] Giuliari, G., Ciussani, T., Perrig, A., & Singla, A. (2021). ICARUS: Attacking low Earth orbit satellite networks. USENIX annual technical conference (USENIX ATC 21), 317-331.

[11] Jiang, Y., Li, X., Zhu, G., Li Hang, Deng, J., Han, K., . . . Zhang, R. (2023). 6G Non-Terrestrial Networks Enabled Low-Altitude Economy: Opportunities and Challenges. arXiv preprint arXiv.

[12] Kendzierskyj, S., Jahankhani, H., & Hussien, O. A. (2024). Space Governance Frameworks and the Role of AI and Quantum Computing. Space Governance, 1-39.

[13] 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.

[14] Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., & Montoya, J. F. (2021). Satellite Communications in the New Space Era: A Survey and Future Challenges. IEEE Communications Surveys and Tutorials, 70-109.

[15] Kosmidis, L., Trompouki, M. M., Solé, M., Suárez, A. Á., & Wolf, J. (2024). Towards a Qualifiable Space Cloud Approach. IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT).

[16] Lamy, A., Le Fevre, C., & Sarli, B. (2012). Analysis of Geostationary Transfer Orbit Long Term Evolution and Lifetime . Journal of Aerospace Engineering, Sciences and Applications, 12-27.

[17] Lin, B., Henry, W., & Dill, R. (2022). Defending Small Satellites from Malicious Cybersecurity Threats. International Conference on Cyber Warfare and Security, 479-488.

[18] Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in New Space Analysis of threats, key enabling technologies and challenges. International Journal of Information Security, 287-311.

[19] Mohammed, A. (2023). Protecting space assets: Cybersecurity challenges and solutions for the final frontier. Baltic Journal of Engineering and Technology, 55-61.

[20] Mohammed, A. (2024). Cybersecurity for Space Systems: Securing Satellites and Communications Against Threats. Innovative Computer Sciences Journal.

[21] Parkinson, B. W. (1997). Origins, Evolution, and Future of Satellite Navigation. Journal of Guidance, Control and Dynamics.

[22] Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight . Journal of Cybersecurity.

[23] Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). Rethinking Satellite Cybersecurity: A System-Level Taxonomy and Longitudinal Analysis. Cryptography and Security .

[24] Radack, S. M. (2003, 8 15). Secure Interconnections for Information Technology Systems. Retrieved from National Institute of Standards and Technology: https://www.nist.gov/publications/secure-interconnections-information-technology-systems

[25] Rocionero-Garcia, J., & Skaikh, S. A. (2024). Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives. Space policy.

[26] 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.

[27] Song, Y., Gnyawali, D., & Qian, L. (2024). From early curiosity to space wide web: The emergence of the small satellite innovation ecosystem. Research Policy.

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

[29] Wang, B., Xiao, J., Dong, R., Piao, C., Guan, Y., Zhao, B., . . . Zhao, Z. (2026). A Comprehensive Literature Review of Cybersecurity in Satellite Networks. Astronautics & Space Science.

[30] Wang, Y., Luo, X., & Wu, X. (2020). Long-term evolution and lifetime analysis of geostationary transfer orbits with solar radiation pressure. Acta Astronautica, 405-420.

[31] Willbold, J., Sciberras, F., Strohmeier, M., & Lenders, V. (2024). Satellite Cybersecurity Reconnaissance: Strategies and their Real-world Evaluation. Aerospace Conference.

[32] Xu, S., Wang, X.-W., & Huang, M. (2018). Software-Defined Next-Generation Satellite Networks: Architecture, Challenges, and Solutions. IEEE Access, 4027-4041.

[33] Yahia, O. B., Erdogan, E., Kurt, G. K., Altunbas, I., & Yanikomeroglu, H. (2022). Optical Satellite Eavesdropping. IEEE Transactions on Vehicular Technology, 10126 - 10131.

[34] Yuan, S., Peng, M., & Sun, Y. (2025). Satellite-Terrestrial Integrated Fog Networks: Architecture, Technologies, and Challenges. IEEE Wireless Communications, 208-215.

[35] Zhu, X., & Jiang, C. (2022). Integrated Satellite-Terrestrial Networks Toward 6G: Architectures, Applications, and Challenges. IEEE 22nd International Conference on Communication Technology (ICCT).