

# A Survey on Satellite Internet Security: Challenges, Principles and Future Trends

Hao Yin<sup>1</sup>, Yuanyu Zhang<sup>2,3</sup>, Shuangrui Zhao<sup>2,3</sup>, Zhiwei Zhang<sup>2,3</sup>, Ji He<sup>2,3</sup>, and Yulong Shen<sup>2,3</sup>

<sup>1</sup>National Key Laboratory for Complex Systems Simulation, Haidian District, Beijing 100080, China

<sup>2</sup>School of Computer Science and Technology, Xidian University,  
266 Xinglong Section of Xifeng Road, Xi'an, Shaanxi 710126, China

<sup>3</sup>Shaanxi Key Laboratory of Network and System Security,  
266 Xinglong Section of Xifeng Road, Xi'an, Shaanxi 710126, China

Satellite Internet is emerging as a critical infrastructure for global connectivity and future 6G networks, but its openness, mobility, predictable topology, and space-ground integration introduce security risks beyond those of terrestrial networks. This survey presents a four-space security taxonomy for Satellite Internet, covering physical entity space, electromagnetic signal space, network information space, and system service space. We further analyze cross-space attack chains in which threats propagate among electromagnetic, cyber, physical, and service domains. Based on this framework, we review ten key defense technologies, including space situational awareness, RF-fingerprinting-enabled signal authenticity authentication, illegal terminal detection and localization, secure space routing, resilient network construction, onboard system security, trusted onboard storage and computing, satellite quantum key distribution, AI security, and cross-space collaborative threat perception and defense. Finally, we discuss open challenges and future directions for each technology, aiming to support the development of integrated, intelligent, and resilient Satellite Internet security architectures.

**Index Terms**—Satellite Internet, electromagnetic security, RF fingerprinting, onboard trusted computing, cross-space attack.

## I. INTRODUCTION

**S**ATELLITE Internet is becoming an essential infrastructure for global broadband connectivity and future ubiquitous communication services. Unlike terrestrial cellular networks, which are constrained by base-station deployment, geographical coverage, and economic cost, Satellite Internet can provide wide-area access over oceans, deserts, mountains, border regions, polar areas, airborne platforms, and other underserved locations. This makes Satellite Internet a key enabler for emergency communications, maritime networking, aviation connectivity, military operations, remote sensing, Internet of Things (IoT), autonomous systems, and future sixth-generation (6G) networks. The 3rd Generation Partnership Project (3GPP) has also incorporated non-terrestrial networks (NTNs) into the 5G evolution, including NR over NTN and IoT over NTN in Release 17, which indicates that satellite access is becoming part of the mainstream cellular ecosystem rather than a separated niche infrastructure [1]–[3].

The rapid deployment of low Earth orbit (LEO) constellations has reshaped the satellite communication ecosystem. Compared with traditional geostationary Earth orbit (GEO) satellite communication systems, LEO satellite networks can

provide lower propagation delay, denser spatial coverage, higher frequency reuse, and more flexible service provisioning; these performance characteristics are discussed in LEO constellation and New Space communication surveys [4]–[6]. Modern Satellite Internet systems are also evolving from simple bent-pipe relays into integrated space information networks that support routing, computing, storage, and intelligent decision-making. ISL-driven routing and topology dynamics are specifically treated in LEO routing and space-network studies [7]–[9], while multi-beam payloads and satellite-terrestrial architectures motivate the use of phased-array, regenerative, and software-defined functions [10]–[12].

However, this evolution also introduces severe security risks. Satellite Internet differs fundamentally from terrestrial networks in terms of openness, mobility, topology, resource constraints, and attack exposure. The openness and boundary-blurring features of satellite Internet are highlighted in recent satellite-security studies [13], [14]. The mobility and handover behavior of LEO access links are treated in LEO access and handover surveys [15]. The predictable nature of orbital motion and the resulting network-topology dynamics are examined in orbital-mechanics and LEO-networking work [9], [16], [17]. Finally, the difficulty of in-orbit maintenance and the need for lifecycle cybersecurity are directly addressed in commercial satellite cybersecurity and space-system security guidance [18], [19].

Existing studies provide important but partial views of this problem. Secure-routing surveys discuss route authentication, trust evaluation, and routing resilience in satellite networks [7], [20]. Space-information-network security work reviews routing anomalies and anomaly detection [21], [22], while satellite-communication security surveys emphasize attacks such as jamming, spoofing, interception, and intrusion [13].

Manuscript received May 13, 2026; revised September 14, 2026.

This work was supported in part by the National Natural Science Foundation of China (No. 62220106004, 92467201), in part by the Fundamental Research Funds for the Central Universities (Grant No. QTZX25080, ZDRC2202), in part by Shaanxi Elite Talent Introduction Program (Youth Project), in part by the Young Talent Fund of Association for Science and Technology in Shaanxi, China, in part by the Natural Science Basic Research Program of Shaanxi Province (2025JC-YBQN-869), in part by the Open Project of Shandong Provincial Key Laboratory of Independent and Reliable Computing Technology and Equipment (No.KT25500400-lab), in part by the Key R&D Program of Shandong Province of China (No.2025CXPT089). Corresponding author: Yuanyu Zhang (email: yyuzhang@xidian.edu.cn), Yulong Shen (email: ylshen@mail.xidian.edu.cn).

Nevertheless, the security of Satellite Internet should not be viewed only as a conventional communication or networking problem. It is a complex cross-domain security problem involving physical space, electromagnetic signal space, network information space, and system service space. An attack may begin from one space and propagate to another. For example, forged satellite signals in the electromagnetic space may induce terminals to access a fake satellite, which then enables network-layer denial of service (DoS), illegal traffic interception, or service-layer information theft. Similarly, network intrusion into a satellite control or management system may lead to malicious command injection, resulting in physical damage through orbit or attitude manipulation.

#### A. Motivation

The motivation of this survey is fourfold. First, Satellite Internet security lacks a unified taxonomy that captures its multi-space nature. Existing classifications often focus separately on physical attacks, signal attacks, network attacks, or system attacks. Such isolated views fail to reveal the coupling among different security domains. Second, cross-space attack chains are becoming increasingly important. The combination of electromagnetic exposure, network openness, onboard intelligence, and physical orbital assets creates new attack paths that cannot be fully understood using traditional Internet security models. Third, future Satellite Internet defense requires integrated security design. Mechanisms such as signal authentication, secure routing, onboard trusted computing, AI security, and space situational awareness should not operate independently. They need to be coordinated under a unified space-ground integrated and cross-space collaborative defense architecture. Fourth, the emergence of software-defined satellites and onboard AI means that security should cover not only confidentiality, integrity, and availability, but also model trustworthiness, computation verifiability, autonomous decision safety, and service continuity.

#### B. Contributions of This Survey

The main contributions of this article are summarized as follows.

- We propose a four-space security taxonomy that classifies Satellite Internet security threats into physical entity space, electromagnetic signal space, network information space, and system service space.
- We analyze how threats propagate across spaces and identify typical attack chains, including electromagnetic-to-network, electromagnetic-to-physical, network-to-physical, network-to-service, and physical-to-network attacks.
- We survey key enabling technologies for Satellite Internet security, covering space situational awareness, signal authenticity authentication, illegal terminal detection, secure routing, resilient networking, onboard system security, trusted computing, satellite quantum key distribution (QKD), AI security, and cross-space collaborative defense.

- We identify open challenges and future research directions, including physical-layer trust anchors, dynamic topology-aware defense, resource-constrained security, cross-space attack modeling, trustworthy onboard AI, and realistic security testbeds.

#### C. Organization of the Article

The remainder of this article is organized as follows. Section II introduces the architecture, trends, and security characteristics of Satellite Internet. Section III presents the four-space threat taxonomy. Section IV analyzes cross-space attack chains and threat propagation mechanisms. Section V reviews key defense technologies. Section VI discusses security design principles. Section VII identifies open challenges and future research directions. Section VIII concludes this article.

#### D. Positioning With Respect to Existing Surveys

Recent surveys on satellite Internet security have evolved from traditional SATCOM architectures toward integrated 5G/6G non-terrestrial networking, secure communications, and cyber resilience. Early studies mainly focused on satellite communication infrastructures, authentication mechanisms, and wireless security vulnerabilities, particularly in SATCOM and global navigation satellite system (GNSS) [23], [24]. With the rise of LEO mega-constellations and NTN-enabled 6G networks, later surveys further investigated satellite-terrestrial convergence, integrated architectures such as space-air-ground integrated networks (SAGIN) and space-air-ground-sea integrated networks (SAGSIN), and the security challenges of large-scale heterogeneous networks [25], [26].

In parallel, security-oriented research has evolved from classical communication threats toward comprehensive protection frameworks for satellite Internet systems. Early studies focused on eavesdropping, spoofing, jamming, replay attacks, and route hijacking in satellite and GNSS communications [23], [27]. Subsequent surveys categorized security mechanisms into cryptography-based and physical-layer approaches, covering authentication, anti-jamming, anti-spoofing, secure routing, and QKD [20], [21], [27], [28]. More recent works further explored lightweight authentication, AI-driven security, blockchain-based trust management, quantum-resistant cryptography, and resilience against real-world cyber incidents in commercial LEO satellite systems [13], [26], [29], [30].

These works provide an important foundation, but they often remain layer-specific or technology-specific. For example, routing surveys concentrate on network-layer path selection, while satellite communication security surveys frequently organize attacks according to the confidentiality-integrity-availability triad. Such classifications are useful but insufficient for Satellite Internet, where attacks may move from the electromagnetic channel into the network, from network control into physical orbit, or from service-layer model compromise into unsafe autonomous decisions. The present survey is positioned as a cross-space systematization: it does not replace existing surveys on routing, physical-layer security, or space-system engineering; instead, it integrates them into a broader threat-propagation view.

Table I summarizes the relationship between this survey and representative prior work. The key distinction is that this article emphasizes four-space threat taxonomy, cross-space attack chains, and defense technologies that jointly cover physical, electromagnetic, network, and service dimensions.

This survey builds upon three research directions. First, studies on satellite Internet architectures, NTN integration, and SAGSIN provide the networking background for understanding satellite–terrestrial convergence and LEO-enabled 5G/6G connectivity [3], [25], [26]. Second, surveys on satellite communication security cover authentication, cryptographic protection, physical-layer security, and communication threats such as spoofing, jamming, eavesdropping, and secure routing [24], [27]–[29]. Third, recent works on LEO resilience, AI-assisted defense, blockchain-based trust management, and real-world cyber incidents offer insights into emerging security challenges in next-generation satellite Internet systems [29], [30].

## II. SATELLITE INTERNET: ARCHITECTURE, TRENDS, AND SECURITY CHARACTERISTICS

### A. Concept and Architecture of Satellite Internet

Satellite Internet refers to an integrated network infrastructure that uses communication satellites, ground stations, inter-satellite links, satellite gateways, and user terminals to provide Internet access and information services [13], [31]. It may involve satellites in different orbital regimes, including LEO, medium Earth orbit (MEO), GEO, and even deep-space nodes. The orbital basis of these systems follows classical astrodynamics, while early LEO studies already showed that time-varying satellite motion makes connectivity and routing fundamentally different from terrestrial networking.

The architectural view adopted here is consistent with classic satellite-network surveys, New-Space communication surveys, constellation-comparison studies, and recent LEO networking analyses.

Fig. 1 presents a layered space–air–ground view of Satellite Internet. Instead of showing only abstract functional blocks, the figure emphasizes the end-to-end operational chain spanning HEO, MEO, LEO, near space, air space, the ground network, and user terminals. In the space domain, the architecture includes navigation systems such as GPS and BDS-3/GLONASS/Galileo, as well as remote-sensing, communication, meteorological, space-situational-awareness, and space-science satellites. It also highlights mobile gateway satellites and inter-satellite links, which together support backhaul connectivity and cross-layer coordination [4], [5].

Below the orbital layers, the architecture further incorporates near-space and aerial platforms, including high-altitude platforms, manned aircraft, and UAVs, which extend coverage for aeronautical, maritime, emergency, and other mobile services. On the ground, TT&C stations, terrestrial 5G/6G access, WiFi/WiMAX systems, core routers and switches, and portable or mobile terminals form the communication and access infrastructure. The service and management side includes the satellite management and control center, satellite control center, mission data processing center, and cloud computing data

center, while the user layer covers IoT devices, smart terminals, SCADA/industrial-control systems, and surveillance and monitoring applications. This representation makes explicit that Satellite Internet is a heterogeneous multi-layer system in which communication, control, sensing, processing, and user services are tightly coupled across space and ground [6], [17].

### B. Evolution Toward Space-Air-Ground-Sea Integrated Networks

Future 6G networks are expected to integrate terrestrial, aerial, maritime, and satellite communication infrastructures [1], [2]. Satellite Internet will play an important role in extending coverage to remote or mobile scenarios where terrestrial base stations are unavailable or economically inefficient. In this context, NTN is an umbrella term for network segments that use satellites, high-altitude platforms, or other non-terrestrial nodes as access nodes or relay nodes [3], [32]. The convergence of satellite networks and terrestrial mobile networks means that authentication, mobility management, session continuity, lawful access, roaming, and security policy enforcement must be redesigned for highly dynamic multi-domain environments [33]. This evolution introduces global seamless coverage, low-latency broadband access through LEO constellations, integration of satellite and terrestrial routing, software-defined payloads, onboard computing and storage, intelligent resource scheduling, and support for mobile terminals such as aircraft, ships, vehicles, and UAVs. At the same time, it blurs traditional network boundaries. Satellite Internet is no longer an isolated space communication system; it becomes part of the global Internet infrastructure. Therefore, vulnerabilities in one segment may affect other segments. For instance, a vulnerability in a ground gateway may expose satellite control or service traffic, while compromised terminals may become entry points for attacks against constellation management infrastructure [32], [34], [35].

### C. Development Trends of LEO Satellite Internet

The development of LEO Satellite Internet shows several major trends.

*Large-scale constellation deployment:* Modern LEO networks rely on hundreds or thousands of satellites to provide continuous global coverage, as discussed in constellation comparison and LEO networking surveys [36]. Large-scale deployment improves coverage and capacity, but also increases the complexity of orbital safety, routing, security monitoring, interference coordination, and constellation lifecycle management [37], [38].

*Lower orbital altitude and reduced latency:* Compared with GEO satellites, LEO satellites operate at much lower altitudes, significantly reducing propagation delay, which has motivated low-latency routing and topology-design studies [9]. This makes LEO Satellite Internet more suitable for interactive services, broadband access, remote control, time-sensitive industrial applications, and integrated 5G/6G services.

*Increased single-satellite capacity:* Advanced payloads, phased-array antennas, high-throughput satellite technologies, and optical ISLs improve single-satellite capacity and network

TABLE I  
POSITIONING OF THIS SURVEY WITH RESPECT TO REPRESENTATIVE SATELLITE INTERNET SECURITY SURVEYS

| Literature Category                               | Representative Focus                                                                                                                                                                | Typical Strength                                                                                                                        | Limitation for Satellite Internet Security                                                                                                            |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Satellite Internet and integrated-network surveys | Satellite Internet architecture, NTN evolution, LEO constellations, and space-air-ground-sea integrated networking [25], [26].                                                      | Provide comprehensive architectural background and clarify the role of satellite networks in future 5G/6G ecosystems.                   | Security is usually discussed at a high level and lacks systematic analysis of attack surfaces and defense mechanisms.                                |
| Authentication and secure communication surveys   | Authentication protocols, access control, cryptographic protection, physical-layer security, anti-spoofing, and quantum-assisted secure communications [24], [28], [29].            | Offer detailed classifications of authentication and secure transmission technologies tailored to satellite communication environments. | Mainly focus on communication confidentiality and identity verification, with limited consideration of system-level and cross-layer security threats. |
| Satellite communication security surveys          | Jamming, spoofing, eavesdropping, routing attacks, malware threats, physical-layer attacks, and corresponding countermeasures in SATCOM systems [13], [27], [30].                   | Provide comprehensive surveys of security threats and defense technologies across different communication layers.                       | Threats are typically analyzed independently and lack a unified perspective on attack propagation across heterogeneous satellite Internet components. |
| Application-oriented and resilience studies       | Security analysis of satellite-enabled services, operational cyber risks, reliability enhancement, intelligent defense, and resilience of large-scale LEO systems [13], [23], [26]. | Highlight practical attack scenarios, emerging cyber incidents, and resilience challenges in commercial satellite deployments.          | Focus on specific applications or operational issues rather than establishing a general security taxonomy for Satellite Internet.                     |
| This survey                                       | Four-space taxonomy, cross-space attack chains, and integrated defense technologies.                                                                                                | Connects physical, electromagnetic, network, and service-space security.                                                                | Requires future refinement with larger empirical datasets and testbeds.                                                                               |

throughput [39]. However, higher capacity also increases the potential impact of a single node compromise or failure.

*Deep integration with terrestrial networks:* Satellite Internet is increasingly integrated with terrestrial mobile networks, cloud infrastructure, and edge computing systems, a trend reflected in 3GPP NTN work and 6G NTN surveys. This integration improves service continuity but also creates new attack surfaces at the satellite-terrestrial interface [40].

*Software-defined and intelligent satellites:* Software-defined payloads and onboard intelligence enable flexible reconfiguration, adaptive routing, and autonomous resource management, but software-defined satellite-networking surveys show that programmability also expands the security responsibility of the control plane. They also introduce software vulnerabilities, AI model security risks, and trusted execution challenges [15], [41].

#### D. Security-Critical Interfaces in Satellite Internet

From a security perspective, the most important characteristic of Satellite Internet is not only that it contains satellites, but that it contains many interfaces with different trust assumptions [13]. The satellite-user interface is exposed to wide-area radio frequency (RF) threats and is the first point where access trust must be established, as satellite communication security surveys repeatedly identify jamming,

spoofing, and interception as primary link-layer risks. The satellite-gateway interface carries user traffic and control-plane messages and is a high-value target for interception, jamming, or traffic manipulation. The inter-satellite interface supports constellation-level routing and is essential for global service continuity, yet it may be affected by pointing errors, optical-link disruption, or compromised routing state. The ground-control interface carries TT&C commands and therefore has direct physical safety implications, which is why commercial satellite cybersecurity guidance treats operations networks and control channels as high-value assets [18], [19]. The cloud/service interface connects satellite infrastructure to terrestrial applications, data centers, and enterprise networks, making it vulnerable to conventional Internet threats.

These interfaces have heterogeneous security requirements. The satellite-user interface requires lightweight authentication, anti-jamming, anti-spoofing, and illegal terminal detection. The gateway interface requires secure tunneling, traffic inspection, gateway hardening, and route validation [42], [43]. The ISL interface requires secure neighbor discovery, link-state authentication, and distributed routing trust. The TT&C interface requires the strongest command authentication, separation of duties, key protection, and anomaly detection. The cloud/service interface requires policy-based access control, data protection, and service-level monitoring. A Satellite In-

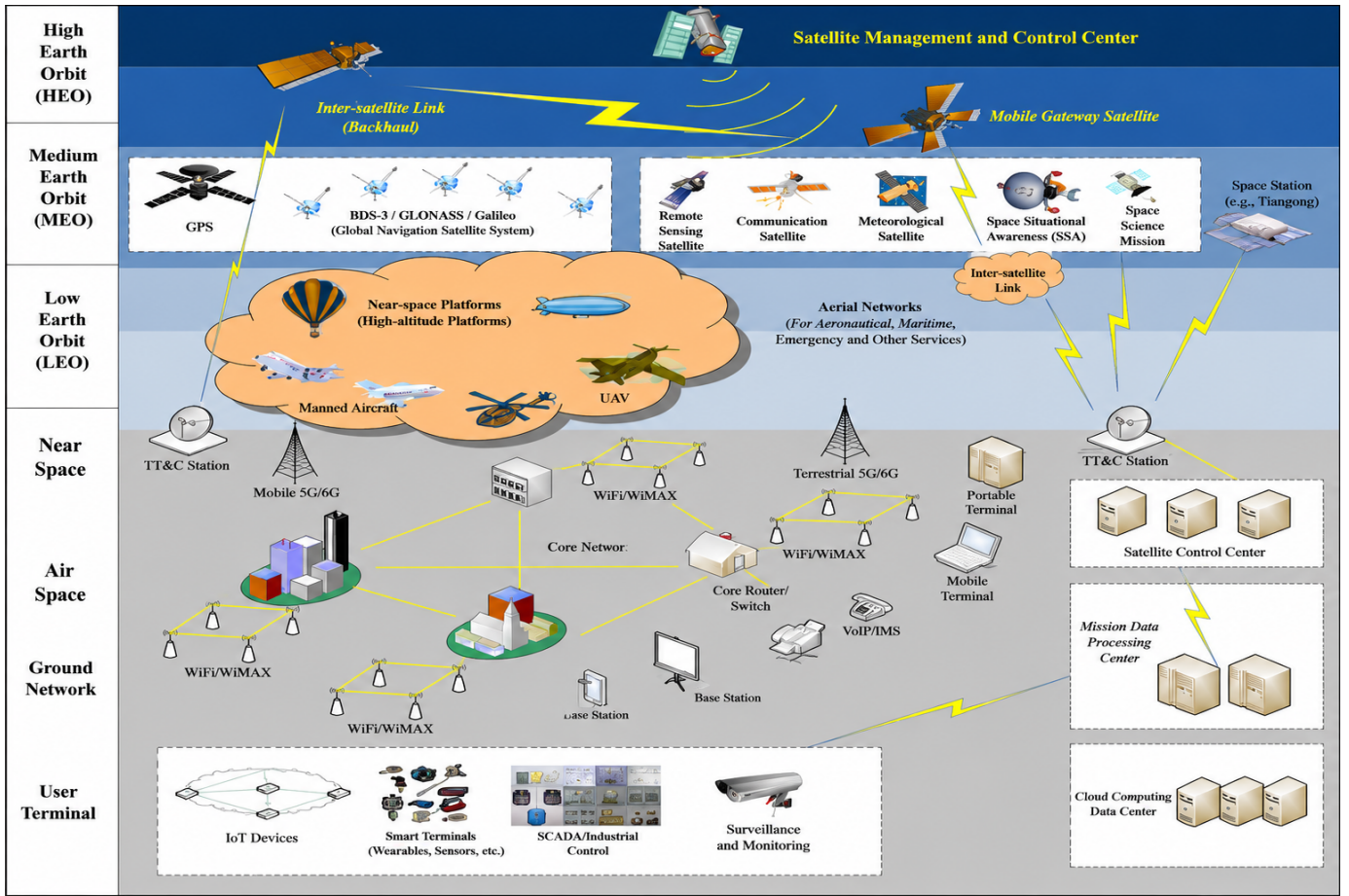


Fig. 1. Space-air-ground Satellite Internet architecture.

ternet security architecture should therefore be interface-aware rather than only node-aware [44], [45].

#### E. Threat Assumptions and Adversary Capabilities

A survey-level security model should distinguish different adversary capabilities [46]. A passive RF adversary can eavesdrop on downlink or uplink signals and perform traffic analysis, as demonstrated by satellite-broadband privacy and infrastructure-security studies. An active RF adversary can jam, replay, or spoof signals. A terminal-level adversary may obtain physical access to user terminals and attempt firmware extraction, fault injection, or credential theft, as illustrated by public Starlink terminal security evaluation work [47], [48]. A network-level adversary may compromise gateways, routing nodes, or management systems. A service-level adversary may poison data, replace AI models, or manipulate computation results. A physical-space adversary may maneuver nearby satellites, damage ground stations, or exploit orbital debris risks [49].

These adversaries differ in cost, visibility, and potential impact. Passive RF eavesdropping may be relatively low-cost but limited by encryption. Signal spoofing requires waveform knowledge and timing control. Terminal compromise requires physical access or supply-chain access, but it may provide a practical bridge to higher-layer networks [50]. Gateway or

control-center compromise is high-impact because it can affect many users or satellites. Physical attacks are expensive but may cause irreversible damage. Cross-space security analysis is needed because an adversary with limited capability in one space may amplify impact by exploiting dependencies in another space [51], [52].

#### F. Unique Security Characteristics

Satellite Internet has several characteristics that distinguish it from terrestrial networks, including the openness, mobility, predictability, and space-ground coupling emphasized in satellite-Internet security surveys [14], [22]. First, satellite access is globally open and may cross national or regional boundaries. Terminals can access satellite networks from remote, maritime, airborne, or border regions. Second, Satellite Internet may provide open access to Internet information and complicate traditional information governance mechanisms [53]. Third, both satellites and terminals may move rapidly, leading to frequent handovers and dynamic links. Fourth, friendly, neutral, and adversarial space networks may coexist in dense orbital regions, increasing the risks of interference, reconnaissance, and strategic confrontation [5], [16]. Fifth, satellite motion follows orbital mechanics and is thus predictable; this property benefits routing but also allows adversaries to anticipate future connectivity windows.

Predictability helps route planning and link scheduling, but it also enables adversaries to forecast link availability, identify high-value relay nodes, and plan targeted disruptions. Table II compares the security characteristics of terrestrial Internet and Satellite Internet.

These characteristics are also highlighted in space-information-network and Satellite Internet security surveys as well as LEO cybersecurity assessments [9], [38].

### III. A FOUR-SPACE SECURITY TAXONOMY FOR SATELLITE INTERNET

Traditional cybersecurity taxonomies are insufficient for Satellite Internet because they usually focus on network-layer threats while underemphasizing electromagnetic exposure, physical orbital assets, and onboard service intelligence. To address this limitation, we classify Satellite Internet threats into four spaces: physical entity space, electromagnetic signal space, network information space, and system service space. This taxonomy reflects the fact that Satellite Internet is not merely a communication network but a space-ground integrated cyber-physical-electromagnetic system. Table III summarizes the threat objects, representative threats, and security goals in each space.

#### A. Physical Entity Space Security

Physical entity space refers to the physical assets and orbital environment of Satellite Internet, including satellites, ground stations, user terminals, launch systems, space debris, and orbital resources [16], [50]. Its security is the foundation of all other spaces because the destruction or degradation of physical assets directly affects electromagnetic coverage, network connectivity, and service availability. The main threats include space debris collision, intentional or accidental close approach, malicious maneuvering, anti-satellite weapons, physical destruction of ground stations, and space environmental hazards such as radiation and solar storms. As LEO constellations grow, the density of objects in orbital shells increases, and the probability of conjunction events becomes a long-term operational concern [54]–[56]. Ground gateways and TT&C facilities are also high-value physical targets because they are the primary interfaces between terrestrial operators and space assets. If a gateway is physically destroyed or disabled, routing, telemetry, service access, and emergency control may be disrupted simultaneously [57], [58].

Physical entity space security therefore requires space situational awareness (SSA), collision avoidance, physical protection of ground facilities, resilient constellation design, and secure lifecycle management. Importantly, physical security cannot be separated from cyber security. A cyber intrusion into a control system may trigger unsafe maneuvers, while physical destruction of a key node may induce network-layer cascading failures [19].

#### B. Electromagnetic Signal Space Security

Electromagnetic signal space refers to the wireless signal environment in which satellite communication, navigation,

telemetry, and control signals are transmitted [59], [60]. This space is one of the most distinctive and vulnerable domains of Satellite Internet. Because satellite beams cover large regions and satellite links rely on open radio-frequency channels, adversaries may intercept, jam, spoof, replay, or analyze signals without physically accessing infrastructure.

Signal jamming is a direct availability attack. It may be broadband, narrowband, reactive, beam-targeted, or protocol-aware. Signal spoofing is often more subtle because it aims to deceive receivers rather than simply deny service [61], [62]. In navigation systems, spoofing can induce false positions; in satellite access networks, forged access signals may trick terminals into connecting to malicious infrastructure. Replay attacks record legitimate signals and retransmit them later or at another location. Interception and traffic analysis threaten confidentiality and privacy, especially when downlink beams cover large geographical regions.

Signal authenticity is therefore a fundamental security problem. If a terminal cannot verify that the received signal originates from a legitimate satellite, upper-layer security mechanisms may be built on a false trust anchor. Cryptographic authentication, navigation message authentication, beam-domain verification, and physical-layer authentication can provide complementary protection [63], [64]. Galileo OSNMA, for instance, represents a major step toward open-service navigation message authentication, although replay-resilience and time-synchronization assumptions still require careful analysis.

The electromagnetic-space taxonomy is anchored in the GNSS security literature, where early work defined spoofing threat models and analyzed receiver requirements for civil anti-spoofing. Civilian spoofing demonstrations and portable spoofing platforms showed that signal-level deception can be practical rather than merely theoretical. Receiver-side detection methods then explored signal-quality monitoring, vestigial-signal analysis, and correlation-domain evidence. UAV and drone demonstrations revealed the physical consequences of electromagnetic deception in mobile platforms. Multipath, receiver-autonomous integrity, and GNSS security surveys provide additional context for distinguishing benign propagation effects from spoofing behavior [65], [66]. Galileo authentication work is directly relevant to signal authenticity, including OSNMA design, receiver guidelines, TESLA-style delayed authentication, and navigation-message authentication analysis. Secure GNSS design and navigation-message authentication studies further clarify the limits of message authentication under replay or time-shifted attacks. Recent anti-spoofing studies also explore consistency tests and multi-receiver or signal-quality methods. Learning-based and tool-supported approaches include grayscale-constellation-image anomaly detection and open-source OSNMA-enabled signal generation. Other studies examine oscillator-stability-based detection and variational-autoencoder RF fingerprinting for GPS anti-spoofing [67].

#### C. Network Information Space Security

Network information space refers to the cyber and network-ing components of Satellite Internet, including protocols, rout-

TABLE II  
COMPARISON BETWEEN TERRESTRIAL INTERNET AND SATELLITE INTERNET SECURITY

| Dimension             | Terrestrial Internet                                                                                      | Satellite Internet                                                                                                                        |
|-----------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Infrastructure        | Mainly fixed terrestrial infrastructure, including base stations, routers, fiber links, and data centers. | Space-ground integrated infrastructure involving satellites, ground gateways, inter-satellite links, user terminals, and control centers. |
| Access boundary       | Access can often be regionally controlled through physical deployment and administrative boundaries.      | Access is globally open because satellite beams can cover remote, maritime, airborne, and cross-border regions.                           |
| Topology              | Relatively stable and administratively manageable.                                                        | Highly dynamic due to satellite motion, yet predictable due to orbital mechanics.                                                         |
| Communication channel | Mixture of wired links and local-area wireless access.                                                    | Wide-area electromagnetic exposure through uplink, downlink, and inter-satellite links.                                                   |
| Maintenance           | Physical maintenance, software patching, and emergency response are comparatively easier.                 | In-orbit maintenance is difficult; patching and recovery are constrained by TT&C links and mission risk.                                  |
| Attack consequence    | Primarily cyber and information-service impact.                                                           | Cyber, electromagnetic, physical, and service impacts may be tightly coupled.                                                             |
| Security objective    | Network confidentiality, integrity, availability, authentication, and access control.                     | Integrated trust, signal authenticity, orbital safety, network resilience, onboard trust, and cross-space defense.                        |

TABLE III  
FOUR-SPACE THREAT TAXONOMY FOR SATELLITE INTERNET

| Space                        | Main Objects                                                                                              | Typical Threats                                                                                                                   | Security Goals                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Physical entity space        | Satellites, ground stations, user terminals, launch infrastructure, orbital assets, space debris.         | Space debris collision, malicious maneuvering, anti-satellite attack, physical destruction of gateways, radiation-induced faults. | Physical safety, survivability, collision avoidance, orbital resilience, secure lifecycle management.    |
| Electromagnetic signal space | Uplink/downlink signals, navigation signals, telemetry and command signals, beams, spectrum resources.    | Jamming, spoofing, replay, interception, spectrum occupation, forged access signals.                                              | Signal authenticity, anti-jamming, anti-spoofing, spectrum controllability, trusted RF access.           |
| Network information space    | Routing protocols, access protocols, inter-satellite links, gateways, ground control networks, terminals. | Unauthorized access, network intrusion, DDoS, routing hijacking, blackhole/wormhole attacks, APT penetration.                     | Identity trust, secure connectivity, secure routing, intrusion resistance, network resilience.           |
| System service space         | Onboard operating systems, computing, storage, AI models, autonomous services, mission systems.           | Data leakage, data tampering, AI model poisoning, model replacement, result falsification, unsafe autonomous decisions.           | Trusted computing, data integrity, verifiable execution, service availability, trustworthy intelligence. |

ing, access control, addressing, gateways, ground networks, ISLs, and management systems [7], [8]. Its threat objects include routing protocols, access protocols, inter-satellite links, gateway networks, ground control networks, user terminal firmware, and orchestration platforms. Major threats include unauthorized access, network intrusion, routing attacks, DDoS, malware injection, compromised firmware updates, and advanced persistent threat (APT) penetration [20], [21]. The 2022 KA-SAT incident illustrates how compromise of satellite communication infrastructure can disrupt large numbers of terminals and have spillover effects beyond the immediate conflict region [68], [69]. The Starlink user-terminal security evaluation further shows that distributed satellite terminals can become attractive attack surfaces, especially when physical access enables fault injection or firmware manipulation [48], [70], [71].

Compared with terrestrial networks, Satellite Internet network security is complicated by dynamic topology, constrained onboard resources, long propagation delay, intermittent links, and difficult patching. Secure routing in LEO networks must consider not only shortest path or latency but also trust, attack exposure, link stability, resource consumption, and mission priorities [72], [73].

#### D. System Service Space Security

System service space refers to the computing, storage, intelligence, and mission-service functions provided by Satellite Internet [74], [75]. As satellites evolve from communication relays to intelligent network nodes, system service security becomes increasingly important. Threat objects include onboard operating systems, onboard processors, storage modules, AI models, autonomous control algorithms, mission planning systems, and service orchestration platforms [76], [77]. The main threats include data leakage, data tampering, AI model poisoning, model replacement, execution result falsification, unsafe autonomous decision-making, and service-level denial [78]. For example, an attacker may tamper with onboard routing tables, poison data used by anomaly detection models, replace a trusted model with a backdoored one, or falsify computation results generated by an onboard edge-computing service [79], [80]. These attacks are especially difficult to handle because satellites may need to operate autonomously for long periods, and emergency maintenance is often constrained [81], [82].

System service security therefore requires secure boot, trusted execution environments, verifiable computing, data lifecycle auditing, secure onboard storage, robust AI, model

integrity verification, and service-level anomaly detection. Unlike traditional cloud or edge systems, onboard service security must be designed under strict constraints in power, computation, radiation tolerance, thermal management, and communication windows [83], [84].

#### E. Interdependence Among the Four Spaces

The four spaces are analytically separable but operationally interdependent [14], [22]. A physical anomaly may change antenna pointing, which degrades electromagnetic link quality, which in turn triggers route switching and service migration. A jamming event may be interpreted as link failure by the routing layer unless RF-layer evidence is shared [85], [86]. A compromised routing update may redirect traffic to a malicious gateway, causing service-layer data leakage. A poisoned AI model may make unsafe routing or maneuvering decisions, creating network or physical consequences [87], [88].

The interdependence argument is consistent with space-information-network security surveys, satellite cyber-risk studies, CCSDS security protocols, and system-resilience engineering guidance.

This interdependence suggests three important design requirements. First, security monitoring should be multi-source and cross-correlated [43]. Second, defense actions should be coordinated to avoid conflicting responses; for example, a route switch caused by suspected jamming should not overload a physically threatened gateway. Third, security metrics should be mission-aware. A small packet-loss increase may be tolerable for best-effort broadband but unacceptable for emergency control, aviation communication, or safety-critical navigation support [45], [77].

#### F. Mapping Threats to Security Properties

Although confidentiality, integrity, and availability remain useful, Satellite Internet requires additional properties [74], [88]. *Authenticity* is needed not only for messages and users but also for signals and physical sources. *Resilience* measures the ability to maintain or recover mission services after attacks or failures [75], [76]. *Verifiability* is essential for onboard computation and AI inference [77], [89]. *Controllability* is necessary for autonomous systems whose decisions may affect physical operations [44], [45]. *Traceability* supports post-incident forensics across space, ground, terminal, and service components. Table IV maps major security properties to the four spaces.

The property mapping extends classic security architecture and control frameworks with space-system security architecture and cryptographic-protocol guidance [85], [86].

### IV. CROSS-SPACE ATTACK CHAINS AND THREAT PROPAGATION

Satellite Internet security cannot be fully understood by analyzing each space independently. In many cases, the most dangerous attacks are cross-space attacks, where the adversary initiates an attack in one space and propagates its impact into another space. Cross-space attacks are particularly important

because Satellite Internet tightly couples physical assets, electromagnetic signals, network protocols, and service functions. Table V summarize representative cross-space attack chains.

#### A. Representative Security Incidents and Their Cross-Space Implications

Publicly reported incidents illustrate why cross-space thinking is necessary [46]. The KA-SAT attack is usually described as a cyber incident because it involved network intrusion and modem disruption, but its impact propagated to real-world communication services and affected users beyond the original conflict theater. The Starlink terminal fault-injection case is often viewed as hardware security research, yet user terminals are part of the distributed satellite-network perimeter and may serve as practical stepping stones for adversaries. GNSS spoofing incidents are electromagnetic attacks, but their consequences may become physical when aircraft, ships, or UAVs follow false positions [47], [48]. These cases show that the entry point and the final impact may belong to different spaces. Operational cybersecurity guidance for commercial satellites treats ground operations, mission assurance, and space-segment protection as connected engineering concerns rather than separate compliance tasks [90]. Satellite eavesdropping and terminal-security studies show that widely deployed user and ground equipment can expose practical attack surfaces [50]. Counterspace assessments provide the physical-security background for proximity, debris, and strategic-interference risks [51]. Public analyses of KA-SAT and AcidRain connect these general concerns to concrete incident chains, while Starlink terminal analyses provide a separate example in which physical access and boot-chain weaknesses expose a satellite user terminal attack surface [52].

#### B. Electromagnetic-to-Network Attacks

In an electromagnetic-to-network attack, the adversary uses forged or manipulated signals to affect network access or network behavior [91], [92]. A typical attack chain is: forged satellite access signal → terminal connects to fake satellite → terminal sends access request → fake satellite drops or manipulates request → network access failure [93], [94]. This attack resembles rogue base station attacks in terrestrial cellular networks, but it is more difficult to detect in satellite environments because satellite signals naturally cover large areas and terminals may not have a nearby trusted infrastructure for verification [95]–[97]. Defense requires satellite signal authenticity authentication, physical-layer identity verification, access signal validation, secure terminal bootstrapping, and multi-source signal consistency checking [98]–[100].

#### C. Electromagnetic-to-Network-to-Service Attacks

This chain is motivated by GNSS authentication, TESLA-based authentication, signal-structure authentication, OSNMA signal generation, and learning-based spoofing-detection studies [101].

In this attack chain, an adversary first uses electromagnetic spoofing to establish a false network connection and then

TABLE IV  
SECURITY PROPERTIES AND EVALUATION DIMENSIONS FOR SATELLITE INTERNET

| Security Property | Meaning in Satellite Internet                                                                                                                                                                              | Representative Threats                                                                                                                                                     | Representative Evaluation Dimensions                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authenticity      | Ensuring that satellites, terminals, signals, commands, routes, data, and service entities are genuine and not forged.                                                                                     | Satellite signal spoofing, forged access signals, illegal terminal impersonation, fake routing information, forged control commands.                                       | Signal authentication accuracy, false acceptance rate, false rejection rate, identity verification latency, robustness against spoofing and replay.                               |
| Integrity         | Ensuring that signals, routing information, onboard data, AI models, commands, and service outputs are not maliciously modified.                                                                           | Navigation message tampering, route manipulation, data modification, AI model replacement, command injection, computation result falsification.                            | Tamper detection probability, integrity verification latency, model verification success rate, data consistency, error propagation impact.                                        |
| Availability      | Ensuring that satellite Internet services remain accessible under attacks, failures, congestion, or extreme environments.                                                                                  | Jamming, DDoS, routing blackhole, satellite node failure, ground gateway disruption, resource exhaustion, physical destruction.                                            | Service continuity ratio, packet delivery ratio, recovery time, network survivability, routing convergence time, anti-jamming performance.                                        |
| Confidentiality   | Protecting user data, control information, telemetry, routing states, and service contents from unauthorized disclosure.                                                                                   | Signal interception, traffic analysis, data leakage, unauthorized terminal access, compromised ground stations, malicious relay nodes.                                     | Encryption strength, leakage probability, eavesdropping resistance, privacy exposure, secure key refresh rate, traffic analysis resistance.                                       |
| Resilience        | Maintaining or rapidly restoring network functions after attacks, failures, or environmental disturbances.                                                                                                 | Space debris collision, node compromise, link interruption, gateway failure, routing attacks, coordinated cross-space attacks.                                             | Fault tolerance, self-healing capability, redundancy level, service recovery time, degraded-mode performance, mission continuity.                                                 |
| Controllability   | Ensuring that satellite Internet entities, resources, access behaviors, routing decisions, onboard execution, and service processes can be constrained, adjusted, isolated, or recovered when risks occur. | Unauthorized access, abnormal terminal behavior, malicious route propagation, compromised onboard tasks, uncontrolled AI decisions, cascading cross-space threats.         | Access revocation time, policy enforcement accuracy, isolation effectiveness, command execution control, resource scheduling controllability, abnormal behavior suppression rate. |
| Traceability      | Ensuring that signal sources, terminal identities, routing paths, data flows, command chains, computation processes, AI model updates, and service behaviors can be recorded, audited, and traced.         | Spoofed signal sources, covert illegal terminals, hidden routing manipulation, data tampering, untraceable command injection, supply-chain compromise, AI model poisoning. | Source localization accuracy, audit log completeness, provenance coverage, attack attribution accuracy, route/path reconstruction accuracy, forensic evidence integrity.          |

TABLE V  
REPRESENTATIVE CROSS-SPACE ATTACK CHAINS

| Attack Chain           | Entry Point                                                   | Propagation Path                                                                    | Final Impact                                                              |
|------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| EM → Network           | Forged satellite access signal                                | Terminal connects to fake satellite; access request is dropped or manipulated.      | Access denial, traffic interception, malicious redirection.               |
| EM → Network → Service | Signal spoofing or rogue satellite relay                      | Malicious session establishment followed by service-layer manipulation.             | Data theft, illegal command injection, service compromise.                |
| EM → Physical          | Navigation spoofing or replay                                 | Receiver computes false position or time; mobile platform follows wrong trajectory. | Route deviation, physical capture, collision, or destruction.             |
| Network → Physical     | Control network intrusion                                     | Malicious command injection changes orbit, attitude, or payload state.              | Physical damage, collision risk, mission failure.                         |
| Network → Service      | Routing attack or gateway compromise                          | Packets are dropped, delayed, duplicated, or redirected to malicious nodes.         | Information leakage, service unavailability, degraded quality of service. |
| Physical → Network     | Physical destruction of satellite, gateway, or ground station | Key node failure fragments topology and overloads remaining paths.                  | Large-scale network disruption and loss of service continuity.            |

exploits the connection to attack service-layer functions [102], [103]. A typical chain is: forged satellite signal → terminal connects to malicious satellite or relay → session establishment → data theft, illegal command injection, or service manipulation [104], [105]. This attack is dangerous because cryptographic protection may be established with the wrong entity if the initial trust anchor is compromised [106], [107]. The key defense principle is to bind physical-layer identity with cryptographic identity and perform continuous verification during the session [108]–[110].

#### D. Electromagnetic-to-Physical Attacks

Navigation-spoofing demonstrations and GNSS countermeasure studies provide direct evidence that electromagnetic deception can create physical-world consequences [90], [109].

Navigation spoofing is a typical electromagnetic-to-physical attack. The adversary forges or replays navigation signals, causing a receiver to compute a false position [67], [102], [108]. This false position may then guide aircraft, ships, vehicles, UAVs, or other mobile platforms toward dangerous or adversary-selected locations [63], [65]. Defense mechanisms include navigation message authentication, anti-replay mecha-

TABLE VI  
REPRESENTATIVE INCIDENTS AND CROSS-SPACE SECURITY IMPLICATIONS

| Incident/Case                        | Primary Entry Space    | Affected Assets                                | Cross-Space Implication                                                        | Lessons                                                                          |
|--------------------------------------|------------------------|------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| KA-SAT cyberattack                   | Network information    | Ground management network and customer modems  | Cyber compromise caused large-scale communication service disruption.          | Ground segment and terminal management are critical parts of satellite security. |
| Starlink terminal fault injection    | Physical/service       | User terminal boot chain and firmware          | Hardware access enabled bypass of secure boot protections.                     | Distributed terminals should be treated as security-sensitive infrastructure.    |
| GNSS spoofing/replay                 | Electromagnetic signal | Navigation receivers and mobile platforms      | RF manipulation can cause false position/time and physical-world consequences. | Signal authenticity and anti-replay are safety-critical.                         |
| Routing manipulation in LEO networks | Network information    | ISLs, gateways, traffic flows                  | Network-layer attacks may cause service leakage or cascading congestion.       | Routing security must be topology-aware and mission-aware.                       |
| Onboard AI model compromise          | System service         | Routing, resource allocation, autonomy modules | Service-layer model compromise may influence network or physical decisions.    | AI security must be integrated into satellite safety assurance.                  |

nisms, multi-sensor fusion, inertial navigation cross-checking, RF fingerprinting of navigation satellites, and anomaly detection in positioning trajectories [64].

#### E. Network-to-Physical Attacks

In network-to-physical attacks, the adversary compromises cyber systems and then causes physical consequences [18], [44], [45]. A typical chain is: intrusion into satellite control network → malicious command injection → orbit or attitude manipulation → physical damage or collision risk [85]–[87]. This type of attack is particularly severe because it transforms a cyber intrusion into a physical-space incident [56], [58]. Strong command authentication, policy-based access control, command behavior verification, independent safety monitors, and secure TT&C architecture are therefore essential [111], [112].

#### F. Network-to-Service and Physical-to-Network Attacks

Routing attacks can directly affect service-layer availability and confidentiality [113], [114]. Blackhole, wormhole, route hijacking, and selective forwarding attacks may cause packet dropping, traffic redirection, information leakage, or service unavailability [7], [72]. Meanwhile, physical destruction of satellites, ground stations, or gateways may cause topology fragmentation and cascading routing failures [8], [20]. These chains show that physical resilience and network resilience are inseparable [21], [68]. A resilient constellation should support redundant routes, dynamic topology reconstruction, service migration, and mission-aware resource scheduling [69], [115].

#### G. Cross-Space Attack Modeling

Cross-space attacks can be modeled as directed graphs in which nodes represent assets, states, or vulnerabilities across different spaces, and edges represent attack propagation paths [116], [117]. A cross-space attack graph may include physical nodes, signal nodes, network nodes, service nodes, dependency edges, attack transition probabilities, defense intervention points, and risk propagation weights [118], [119].

Such models can support threat prediction, attack-path discovery, risk quantification, and optimal defense planning [14], [22]. Compared with conventional cyber attack graphs, cross-space graphs must model physical dynamics, orbital constraints, link schedules, electromagnetic coverage, and mission dependencies [43], [50].

Attack-chain modeling can borrow from classical attack-graph generation, logic-based security analysis, scalable attack-graph construction, and Bayesian attack-graph risk management [19], [51].

### V. KEY DEFENSE TECHNOLOGIES

This section follows the technical roadmap emphasized by the source report: instead of expanding the survey by adding loosely related security topics, we organize the defense landscape around ten key technologies that are directly associated with Satellite Internet deployment and operation. These technologies are not independent modules. Space situational awareness protects the physical basis of the constellation; RF-fingerprinting-enabled signal authenticity authentication and illegal terminal detection secure the electromagnetic entrance; secure routing and resilient networking maintain network continuity; onboard system security and trusted storage/computing protect the service foundation; satellite quantum key distribution strengthens long-distance key establishment; AI security protects the intelligence engine; and cross-space collaborative threat perception connects all spaces into an integrated defense loop. Fig. 2 and Table VII summarize this focused ten-technology landscape.

#### A. Space Situational Awareness

Space situational awareness (SSA) is the first line of defense for the physical entity space of Satellite Internet [16], [50]. In a dense LEO constellation, the security of communication services depends on the continued physical availability of satellites, orbital resources, ground gateways, and supporting infrastructure [120]. SSA therefore goes beyond traditional orbit catalog maintenance. For Satellite Internet, it must support continuous target detection, target identification, target

TABLE VII  
TEN KEY DEFENSE TECHNOLOGIES FOR SATELLITE INTERNET SECURITY

| Technology                                                   | Primary Space              | Core Function                                                                                  | Key Technical Focus                                                                                                                             |
|--------------------------------------------------------------|----------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Space situational awareness                                  | Physical                   | Detect, identify, track, and assess satellites, debris, and abnormal maneuvers.                | Multi-source observation fusion, orbit prediction, collision warning, threat attribution, and decision support.                                 |
| RF-fingerprinting-enabled signal authenticity authentication | Electromagnetic            | Verify whether received satellite signals originate from legitimate satellites.                | Feature extraction, Doppler/channel compensation, fingerprint database management, replay/spoofing discrimination, and anti-imitation analysis. |
| Illegal terminal detection and localization                  | Electromagnetic or Network | Discover unauthorized terminals and estimate their locations.                                  | Spectrum sensing, modulation/protocol recognition, directional behavior analysis, TDOA/FDOA/AOA fusion, and beam-domain localization.           |
| Space secure routing                                         | Network                    | Maintain trustworthy data forwarding under dynamic topology and attacks.                       | Attack-aware routing, trust evaluation, link-state protection, autonomous route decision, and route recovery.                                   |
| Large-scale resilient network construction                   | Network/Physical           | Preserve service continuity under failures, attacks, congestion, and node loss.                | Redundant topology, self-healing, service migration, mission-aware recovery, and cascading-failure containment.                                 |
| Onboard system security                                      | System service             | Protect satellite hardware, firmware, operating systems, and update mechanisms.                | Hardware root of trust, secure boot, trusted OS, radiation tolerance, dual-image backup, and authenticated remote repair.                       |
| Onboard trusted storage and computing                        | System service             | Ensure onboard data integrity, computation correctness, and lifecycle auditability.            | Trusted execution, integrity verification, secure databases, verifiable computing, and auditable data lifecycle.                                |
| Satellite quantum key distribution                           | Network/Service            | Provide long-distance high-security key establishment for critical links.                      | Satellite-ground QKD, trusted relay architecture, key management, integration with classical security protocols, and operational feasibility.   |
| Satellite Internet AI security                               | System service/All         | Protect AI models used for routing, perception, resource allocation, and autonomous operation. | Data poisoning defense, model integrity, secure deployment, robust inference, explainability, and trusted model updates.                        |
| Cross-space collaborative threat perception and defense      | All                        | Correlate multi-space evidence and coordinate defense actions.                                 | Threat representation, attack-chain reasoning, risk propagation modeling, multi-source fusion, and coordinated response.                        |

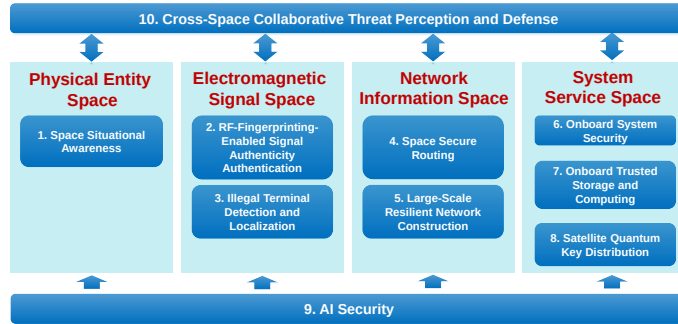


Fig. 2. Ten key security technologies for Satellite Internet.

tracking, situation analysis, and warning-based decision support [121]. The monitored objects include operational satellites, inactive spacecraft, rocket bodies, small debris, unknown targets, and potentially adversarial satellites that may conduct proximity operations or abnormal maneuvers [51], [56]. A complete SSA pipeline contains several tightly coupled functions. Target detection discovers objects in LEO, MEO, GEO, and other relevant orbital regions by using optical telescopes, radar, radio monitoring, laser ranging, and other measurement resources [122]. Target identification classifies whether an object is a known communication satellite, navigation satellite,

reconnaissance satellite, inactive object, debris fragment, or unknown maneuvering target. Target tracking estimates and continuously updates orbital parameters, while short-term and long-term prediction provides future positions and conjunction probabilities [57], [58]. Situation analysis then evaluates collision risk, abnormal maneuver intention, orbital congestion, and potential service impact. Finally, warning and decision support translate risk estimates into operational actions, such as maneuver avoidance, beam switching, link rerouting, frequency rescheduling, or temporary service degradation.

For security surveys, the key point is that SSA should be linked with cyber and network security rather than treated as a purely aerospace function [123], [124]. A physical threat may become a network threat when a key satellite, inter-satellite link, or gateway is lost [19], [111]. Conversely, a cyber intrusion may produce abnormal physical behavior if malicious commands affect satellite attitude or orbit control. Future SSA for Satellite Internet should therefore provide not only object-level warnings but also mission-level impact estimation. For example, a predicted collision with a relay satellite should be translated into affected beams, disconnected terminals, vulnerable routing paths, and service recovery plans [18]. Such coupling is essential for cross-space defense.

### B. RF-Fingerprinting-Enabled Signal Authenticity Authentication

Signal authenticity authentication is a foundational defense technology in the electromagnetic signal space [125], [126]. In Satellite Internet, the terminal must first decide whether the received satellite signal is genuine before it can safely perform network access, key negotiation, routing participation, or service interaction. If this first trust anchor is wrong, higher-layer cryptographic mechanisms may protect a connection with the wrong entity. Therefore, signal authenticity should be viewed as the source-side defense that prevents electromagnetic attacks from becoming network and service attacks. RF fingerprinting is a key technical path for satellite signal authenticity authentication. Unlike message-level authentication, which verifies whether the received bits carry a valid signature or authentication code, RF fingerprinting aims to determine whether the physical transmitter has the expected hardware characteristics. Satellite transmitters contain oscillators, mixers, power amplifiers, filters, clocks, digital-to-analog converters, antennas, and other components [127], [128]. Their imperfections generate device-specific signal features, such as carrier frequency offset, phase noise, I/Q imbalance, power-amplifier nonlinearity, transient behavior, modulation error patterns, and spectral regrowth. These features can be extracted from received signals and compared with a stored satellite fingerprint database, as illustrated by recent GNSS and satellite-authentication studies based on oscillator stability, variational autoencoders, and 3D convolutional RF fingerprinting.

A typical RF-fingerprinting-enabled authentication procedure includes signal acquisition, synchronization, Doppler compensation, channel normalization, feature extraction, fingerprint matching, and decision output. Besides transmitter-fingerprint features, image-based learning representations such as grayscale constellation images have also been explored for GPS spoofing detection. The key difficulty is to separate transmitter-induced features from channel-induced and motion-induced distortions. In LEO scenarios, Doppler shift varies quickly, link geometry changes continuously, and received signal strength may fluctuate due to beam switching, atmospheric effects, terminal motion, and multipath [129], [130]. If these effects are not compensated, the extracted fingerprint may reflect the channel rather than the satellite. Therefore, robust feature design should focus on hardware-stable components while reducing sensitivity to propagation conditions.

Another central issue is non-forgability. An attacker may attempt to emulate the waveform, replay a captured signal, or synthesize features that resemble a legitimate satellite. RF fingerprinting must therefore be evaluated not only by classification accuracy but also by adversarial imitation difficulty. Useful metrics include intra-satellite stability, inter-satellite separability, spoofing detection probability, false alarm rate, replay discrimination capability, and minimum feature-space distance under manufacturing tolerance and receiver noise. In this sense, RF fingerprinting should be integrated with cryptographic signal authentication rather than used as a standalone replacement. A strong design binds physical-layer

identity with message-level identity, so that a valid cryptographic message must also originate from a transmitter whose RF fingerprint is consistent with the expected satellite [131], [132]. IoT and deep-learning fingerprinting studies provide practical evidence that RF identities can be learned from commodity wireless signals. Satellite and GNSS transmitter-identification studies then adapt this idea to space signals, where oscillator stability, Doppler dynamics, and long-distance propagation are central concerns. RF machine-learning surveys and modulation-recognition work help explain why feature representation and dataset shift matter for realistic authentication systems. Classical transient-based approaches remain relevant because transmitter turn-on behavior, modulation errors, and analog-front-end imperfections often contain stable device information. Earlier emitter-identification studies based on transient extraction and exploitation provide useful methodological precedents for satellite fingerprint design. More recent learning-based radio-identification work further motivates robust feature extraction under channel variation and adversarial conditions [133], [134].

### C. Illegal Terminal Detection and Localization

Satellite Internet coverage crosses geographical boundaries. This property is beneficial for global access but also enables unauthorized or illegal terminals to communicate through foreign satellite networks, especially in border, maritime, desert, or mountainous areas [42], [49]. Illegal terminals may support covert communication, data leakage, intelligence collection, or unauthorized Internet access. Therefore, terminal detection and localization are important security functions in the electromagnetic and network spaces.

Illegal-terminal monitoring is related to satellite-broadband measurement, SATCOM terminal security, RF fingerprinting of rogue devices, and LEO/SATCOM cybersecurity assessments.

The first task is detection. Spectrum sensing can identify suspicious uplink emissions by monitoring frequency occupancy, time activity, bandwidth, power, and beam direction [24]. Modulation and protocol recognition can infer whether an observed signal belongs to a known satellite system or an unauthorized access pattern. Directional communication behavior analysis is particularly useful because many satellite terminals use phased arrays or directional antennas. Their pointing direction, transmission timing, burst structure, and Doppler behavior may reveal whether they are communicating with domestic, foreign, or suspicious satellite resources [135].

The second task is localization. Common approaches include time difference of arrival (TDOA), frequency difference of arrival (FDOA), angle of arrival (AOA), received signal strength, polarization features, and multi-station direction finding [136]–[138]. Beam-domain localization can use satellite beam coverage, antenna gain patterns, and access logs to constrain the terminal position. In practice, localization is difficult because illegal terminals may transmit intermittently, use low power, operate under terrain blockage, hide in urban clutter, or employ mobility to avoid detection. Sparse monitoring infrastructure further limits localization accuracy.

Therefore, effective solutions need to fuse RF measurements, satellite access records, geospatial information, and behavioral models [139]–[141].

Illegal terminal defense should also be connected with access control. Detection alone is insufficient if the system cannot revoke access, isolate suspicious sessions, or provide evidence for operational response. A practical architecture should combine electromagnetic monitoring, satellite-network logs, terminal identity management, and policy enforcement. When suspicious activity is detected, the system may perform additional challenge-response authentication, reduce service privileges, switch beams, collect more measurements, or coordinate with ground monitoring stations for localization [134], [142].

#### D. Space Secure Routing

Routing is the nervous system of Satellite Internet. Early and modern satellite-routing studies show that LEO forwarding is shaped by predictable contact windows, changing link availability, and topology-dependent delay [31], [71]. LEO satellites move rapidly, inter-satellite links change according to orbital geometry, and gateway visibility varies over time. In such a dynamic environment, routing must not only optimize delay, throughput, and load balance but also resist malicious manipulation. Routing attacks may include blackhole attacks, wormhole attacks, route hijacking, false link-state advertisement, selective forwarding, topology poisoning, and DDoS-induced congestion. Because satellite topology is predictable, an adversary can plan attacks against future key nodes or links with high routing centrality [68], [69]. Secure routing should provide three capabilities. The first is route-state protection, because secure-routing surveys for satellite and space information networks emphasize false route advertisements, malicious relays, and anomaly-aware routing as core threats. First, route information must be authenticated and integrity-protected. Satellites should not blindly trust link-state updates, gateway advertisements, or neighbor reports. Second, route selection should be attack-aware. If a node, link, beam, or gateway is suspected to be compromised or jammed, routing should avoid it when possible, even if the alternative path has higher latency [7], [115]. Third, routing recovery should be autonomous. Ground-based route repair may be too slow under fast-changing topology or attack conditions, so satellites need local decision capability under predefined safety and security policies.

A key research issue is the tradeoff between security and performance. Contact-graph and delay/disruption-tolerant networking studies are relevant when links are intermittent or scheduled rather than continuously available [8], [20]. The shortest path may not be the safest path. The most trustworthy path may consume more scarce satellite resources. Multi-path routing can improve resilience but may increase overhead and expose traffic to more nodes. Secure routing metrics therefore need to combine propagation delay, queueing delay, link reliability, trust score, attack probability, mission priority, and remaining energy or processing resources. Secure routing should also interact with SSA and signal monitoring. For

example, if SSA predicts a high-risk physical event or RF monitoring detects jamming in a certain region, the routing layer should proactively reconfigure paths before service collapses [21], [72].

#### E. Large-Scale Resilient Network Construction

Resilience is the ability of Satellite Internet to continue, degrade gracefully, and recover rapidly under faults, attacks, congestion, and environmental disturbances [73], [113]. Cyber-resilience engineering guidance is useful here because it emphasizes anticipation, withstanding, recovery, and adaptation rather than simple perimeter protection. In large-scale LEO constellations, resilience is not simply redundancy. It requires a systematic design that links constellation topology, inter-satellite links, gateway placement, resource scheduling, service migration, and defense response [9], [114]. Resilient network construction includes three layers of capability. The first is structural resilience. The constellation should avoid excessive dependence on single nodes, single orbital planes, or a small number of gateways. Redundant inter-satellite links, diverse ground gateways, and multi-path connectivity can reduce the impact of node failure [143]–[145]. The second is operational resilience. When a link is jammed, a satellite fails, or a gateway is attacked, the network should dynamically reconstruct topology, reroute traffic, migrate services, and allocate resources according to mission priority [37], [38]. The third is active defense resilience. The network should detect early signs of attacks, isolate compromised nodes, limit attack propagation, and restore normal operation after containment [146].

A special challenge is cascading failure. Because Satellite Internet routing and service dependencies are time-varying, the failure of a physically small number of nodes may produce disproportionate service impact if those nodes are temporarily central in the topology [39], [77]. Resilience analysis should therefore be time-dependent and mission-aware. The same satellite may be non-critical at one moment and critical at another because of orbital position, gateway visibility, or traffic concentration. Resilient design should include predictive risk warning, dynamic backup selection, and service-level continuity planning [147], [148].

#### F. Onboard System Security

Onboard system security protects the satellite platform, payload, firmware, operating system, onboard applications, and update mechanisms [44], [45]. Unlike ground systems, satellites are difficult or impossible to physically repair after launch. They operate under radiation, thermal variation, limited power, and long lifecycle constraints. A security failure may therefore persist for years or cause irreversible mission impact.

Onboard system security is guided by CCSDS space-data-system security standards, NIST trustworthy-system engineering, and space-system cybersecurity analyses [85], [86].

A secure onboard system should begin with a hardware root of trust. Secure boot verifies each stage of firmware and software before execution, preventing unauthorized code

from running. Chain-of-trust mechanisms should extend from boot ROM to bootloader, operating system, payload software, and mission applications [58], [149], [150]. A trusted operating system should provide process isolation, memory protection, access control, and secure inter-process communication. Safety-critical functions, such as attitude control, TT&C command execution, and payload reconfiguration, should be isolated from less trusted service functions [19], [87].

Satellite-specific issues make onboard security harder. Radiation may cause bit flips that resemble software faults or even security anomalies. Secure systems therefore need both fault tolerance and attack detection. Dual-image backup and rollback mechanisms can support recovery from corrupted updates, but they must prevent downgrade attacks. Authenticated remote repair is necessary because ground operators may need to patch vulnerabilities after launch [74], [76]. However, the update channel itself is a high-value target. Update packages should be signed, version-controlled, integrity-checked, and protected against replay.

Supply-chain assurance is also important. Satellite hardware and software may involve many vendors and long development cycles. Vulnerabilities may be introduced before launch and remain hidden until in-orbit operation. Therefore, onboard system security should cover the full lifecycle: design, manufacturing, integration, testing, launch, operation, update, and decommissioning [111].

#### *G. Onboard Trusted Storage and Computing*

As satellites evolve from communication relays to computing and storage nodes, onboard trusted storage and computing become central to system service space security [76], [89]. Satellites may process routing decisions, sensing data, user traffic, AI inference results, caching content, and mission commands [151]. If data are tampered with or computation results are forged, the satellite may provide incorrect services even when the communication link is available.

Trusted onboard data and computation require key-management, cryptographic-algorithm, secure-data-link, and secure-systems engineering foundations [152], [153].

Trusted storage aims to provide confidentiality, integrity, freshness, and auditability [74], [77]. Data stored onboard should be protected against unauthorized reading, modification, deletion, and rollback. Integrity verification can detect whether mission data, routing tables, AI models, logs, or configuration files have been modified. Secure databases and append-only logs can support post-event forensics and lifecycle auditing. Freshness protection is particularly important because replayed old configuration data may bypass simple integrity checks [75], [87].

Trusted computing focuses on the correctness and trustworthiness of execution. Trusted execution environments can isolate sensitive computation from untrusted software. Remote attestation allows ground stations or peer satellites to verify that a satellite is running expected software before trusting its outputs. Verifiable computing can allow a resource-limited verifier to check computation results without repeating the entire computation [44], [45]. However, onboard resource

constraints make heavyweight trusted computing difficult. Future designs should develop lightweight attestation, selective verification, hardware-assisted isolation, and mission-specific trusted execution policies.

The boundary between onboard system security and trusted computing is subtle. Onboard system security protects the platform itself; trusted storage and computing protect the data and computational services running on top of that platform [19], [85]. Both are necessary for service trustworthiness.

#### *H. Satellite Quantum Key Distribution*

Satellite quantum key distribution (QKD) addresses the long-distance key establishment problem [154], [155]. Conventional public-key cryptography depends on mathematical assumptions that may be weakened by future quantum computing. Fiber-based QKD can provide strong security but is limited by distance and deployment cost. Satellite QKD can extend secure key distribution across regions, countries, and continents by using free-space optical links between satellites and ground stations [156]. In the context of Satellite Internet security, QKD should be viewed as a high-assurance key distribution mechanism for critical links rather than a universal replacement for all cryptographic protocols. It may support secure satellite-ground links, inter-ground-station key relay, backbone key refresh, and high-value mission communications. QKD-generated keys still need to be integrated with authentication, key management, access control, and classical encryption systems [157], [158]. Therefore, the system-level problem is not only how to distribute quantum keys but also how to incorporate them into operational Satellite Internet architectures.

Several challenges remain. Optical links require accurate pointing, acquisition, and tracking. Atmospheric turbulence, weather, daylight background noise, and satellite pass duration affect key rate and availability. Trusted-relay architectures introduce trust assumptions at satellite or ground nodes. Integration with large-scale LEO networking requires scheduling QKD sessions, storing keys, refreshing keys, and allocating scarce optical resources [159], [160]. Therefore, satellite QKD is most suitable for critical services and high-value links where the security gain justifies operational complexity.

The technology combines two traditions: physical-layer security and quantum cryptography. Wiretap-channel and secret-key-agreement theory explain why physical channels can support secure key establishment, while satellite QKD experiments demonstrate that free-space quantum links can extend secure key distribution beyond fiber-limited distances [161], [162].

#### *I. Satellite Internet AI Security*

AI is becoming an enabling technology for Satellite Internet. It may support spectrum sensing, anomaly detection, routing optimization, beam management, resource allocation, collision avoidance, illegal terminal detection, and autonomous fault recovery [163], [164]. However, once AI participates in security-critical decisions, its own security becomes part of the Satellite Internet security foundation. AI security should

be considered across training, deployment, and inference. In the training stage, data poisoning may corrupt models used for anomaly detection or routing decisions [165], [166]. Backdoor attacks may cause a model to behave normally under most inputs but fail under attacker-chosen triggers. In the deployment stage, a model may be replaced, modified, stolen, or reverse-engineered. In the inference stage, adversarial inputs may manipulate decisions, and repeated queries may leak model information [79], [167]. These problems are amplified onboard because computing resources are limited and human intervention may be delayed.

A secure AI pipeline should include data provenance, training-data anomaly detection, model auditing, model signature verification, secure model storage, trusted inference, and monitored model update. For onboard AI, explainability is also important. Operators need to understand why an AI system recommends a route change, beam switch, maneuver warning, or access denial. AI should assist defense decision-making but should not become an unconstrained autonomous authority in safety-critical operations [81], [168]. A practical design is to combine AI-based perception with rule-based safety constraints and auditable human-overridable policies.

The technical baseline for AI security includes adversarial-example attacks, robust optimization, poisoning, and backdoor threats. These threats are relevant to Satellite Internet because learning models may be embedded in resource allocation, handover, spectrum sensing, anomaly detection, and autonomous decision loops [80], [169].

#### *J. Cross-Space Collaborative Threat Perception and Defense*

The tenth key technology is the integrator of the previous nine. Cross-space collaborative threat perception and defense aims to connect physical, electromagnetic, network, and service evidence into a unified risk picture [116], [117], [170]. Without this capability, each defense mechanism may see only a fragment of an attack. For example, RF monitoring may observe abnormal signals, the routing layer may observe path degradation, and onboard logs may show service anomalies. Individually, each event may look ambiguous; together, they may reveal an electromagnetic-to-network-to-service attack chain [22], [119].

Cross-space perception requires combining attack-graph reasoning with space-security incident analysis and cyber-resilience engineering [171], [172].

A cross-space defense system should include threat representation, multi-source monitoring, attack-path reasoning, risk propagation assessment, and coordinated response. This mirrors the way cyber-resilience and space-cybersecurity guidance connect detection, response, recovery, and mission assurance rather than treating alerts as independent events [14], [43]. Threat representation defines common objects, relationships, states, and events across spaces. Multi-source monitoring collects SSA data, spectrum observations, network traffic, access logs, terminal behavior, onboard system logs, service status, and AI model integrity evidence. Attack-path reasoning infers whether these observations form a plausible attack chain. Risk

propagation assessment estimates how a local event may affect future topology, services, and missions [50], [51]. Coordinated response then chooses actions such as signal authentication escalation, terminal isolation, route reconfiguration, service migration, model rollback, or physical maneuver support.

The main difficulty is timeliness and trust. Cross-space defense must operate under incomplete and uncertain data. It must avoid both underreaction and overreaction, because unnecessary route changes or service isolation can also harm mission continuity. Therefore, future systems should combine probabilistic reasoning, graph-based attack models, digital-twin simulation, and operator-in-the-loop decision support [19], [56].

## VI. SECURITY DESIGN PRINCIPLES

Future Satellite Internet security should be guided by three principles: space-ground integrated design, cross-space collaborative design, and intelligence-driven design. These principles are not independent; they together define a system-level defense philosophy for Satellite Internet.

### *A. Space-Ground Integrated Security Design*

Satellite Internet integrates satellites, ground stations, gateways, terrestrial networks, cloud services, and user terminals [88], [173]. Security mechanisms should therefore be designed in an integrated manner. Terrestrial security mechanisms cannot be directly transplanted to satellite networks due to delay, mobility, resource constraints, and dynamic topology. However, satellite and terrestrial security mechanisms must be compatible. For example, terrestrial zero-trust access control can inspire continuous identity verification for satellite terminals, but trust evaluation must incorporate satellite-specific context such as beam coverage, Doppler trajectory, terminal location, and link schedule [174].

The standards basis for such integration is necessarily multi-source. ITU security architecture and policy-management recommendations provide a general end-to-end framework for organizing heterogeneous security functions, while fixed-mobile-satellite convergence and IMT vision documents motivate the integration of terrestrial and satellite domains. IoT gateway and device-security recommendations are relevant to satellite terminals and edge gateways. At the cellular side, 3GPP NTN reports and 5G system specifications define the assumptions behind satellite access, mobility, control-plane exposure, and security procedures [175]. Radio-access and NG-RAN specifications clarify where satellite links interact with RRC, radio-resource control, and access-network architecture. For space-data systems, CCSDS security documents define protocol, data-link, cryptographic, and architecture-level mechanisms that are directly relevant to TT&C and mission-data protection. NIST risk-management, security-control, system-security-engineering, resilience, key-management, and post-quantum-transition documents provide complementary engineering baselines for lifecycle assurance [176].

Space-ground integrated security should also defend against bidirectional attack propagation. Attacks may propagate from

ground networks to satellites through compromised gateways or TT&C systems, and from satellite networks to ground services through malicious traffic redirection or compromised user terminals. Integrated monitoring should combine satellite telemetry, ground network logs, spectrum data, access control records, and user behavior. Security orchestration should be able to isolate compromised gateways, revoke terminal credentials, change routing policies, and trigger satellite-side safeguards [147].

### B. Cross-Space Collaborative Security Design

Traditional security boundaries are often separated by domain. Satellite Internet requires coordinated defense across four spaces [76], [87]. In physical entity space, security goals include collision avoidance, physical isolation, trusted location, and survivable assets [44], [45]. In electromagnetic signal space, goals include signal authenticity, spectrum controllability, anti-jamming, anti-spoofing, and interference detection. In network information space, goals include trusted identities, secure links, controllable access, secure routing, and intrusion resistance [85], [86]. In system service space, goals include data trustworthiness, behavior controllability, service availability, and trustworthy intelligence.

Cross-space design requires shared data models and interfaces. Security-architecture recommendations and space-system cybersecurity guidance are useful baselines, but they must be extended to represent dependencies among RF, routing, onboard software, and mission services. A jamming event should be visible not only to RF monitoring systems but also to routing, service scheduling, and mission risk assessment. A suspected routing attack should trigger checks on electromagnetic anomalies and terminal behavior [75], [77]. A physical conjunction warning should inform network topology prediction and service migration. This requires a collaborative security architecture rather than isolated security products [18], [74].

### C. Intelligence-Driven Security Design

AI can significantly enhance Satellite Internet security by improving risk perception, threat prediction, decision-making, and adaptive response, especially where learning is already being explored for NTN resource management, handover, and software-defined satellite networking [12], [177]. Intelligent situation awareness can fuse heterogeneous data from multiple spaces and identify abnormal patterns. Intelligent attack detection can recognize complex attacks that span layers and domains [32], [35]. Intelligent decision response can recommend route isolation, link switching, beam adjustment, access revocation, or service migration. Intelligent policy evolution can update security strategies based on observed threats and mission requirements [79], [169].

Security large models may support threat intelligence analysis, attack-chain reasoning, vulnerability discovery, and automated defense planning [178], [179]. However, their own trustworthiness must also be ensured. If a large model is used as a security assistant, its recommendations should be auditable, constrained by policy, and validated against formal

safety rules. For critical satellite operations, human-in-the-loop control and verifiable decision logic remain necessary [180].

## VII. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section is reorganized according to the ten key technologies rather than adding a large number of loosely connected future topics. Each direction corresponds to one technology in Section V. The purpose is to deepen the technical roadmap implied by the report and to make the survey more focused: the open questions are not independent slogans but unresolved problems that must be addressed for each key defense capability.

### A. Space Situational Awareness: From Object Tracking to Security-Aware Mission Impact Prediction

Traditional SSA focuses on object cataloging, orbit determination, conjunction analysis, and collision warning, but security-oriented space assessments also emphasize cyber-physical risks, counterspace capabilities, and mission impact [16], [50]. For Satellite Internet security, this is necessary but not sufficient. The open challenge is to evolve SSA from object-centric awareness to mission-centric and security-aware awareness. A predicted conjunction should not only produce a collision probability; it should also indicate which beams, inter-satellite links, gateways, users, routes, and services may be affected if a maneuver or failure occurs. Similarly, an abnormal proximity operation should be assessed not only as an orbital event but also as a potential precursor to interference, eavesdropping, inspection, collision, or service disruption [19], [51].

Future SSA research should connect orbital-state prediction with mission-impact analysis, drawing on astrodynamics, counterspace assessment, and space-system cybersecurity research. Future research should integrate orbital mechanics with network topology, service dependency, and threat intelligence. A promising direction is security-aware SSA digital modeling, in which orbital states, network states, and mission states are jointly represented. Such models can support questions such as: Which satellites are physically critical at a given time? Which orbital events may trigger cascading routing failures? How should maneuver avoidance be coordinated with communication continuity? How can cyber evidence, such as abnormal command behavior, be correlated with physical maneuver anomalies? These questions define the next generation of SSA for Satellite Internet security [18], [56].

### B. RF-Fingerprinting-Enabled Signal Authenticity: From Classification Accuracy to Non-Forgeability

Most RF fingerprinting studies emphasize identification accuracy under controlled datasets [181], [182]. For satellite signal authenticity authentication, this is only the starting point. The deeper challenge is to establish whether RF fingerprints remain stable, distinguishable, and difficult to forge under realistic LEO conditions [183]. The feature distribution of a satellite may be affected by Doppler shift, beam switching, channel fading, temperature, hardware aging, payload

reconfiguration, receiver type, and preprocessing algorithms. A classifier with high accuracy in one dataset may fail when deployment conditions change.

Future RF-authentication work should combine classic RF identification, modern deep-learning RF fingerprinting, and satellite/GNSS anti-spoofing studies [125], [184]. Future work should shift from black-box classification to mechanism-aware fingerprint modeling. Researchers should identify which RF impairments are mainly caused by satellite hardware, quantify how they are transformed by propagation and receiver chains, and determine which features can support long-term authentication. Security evaluation should include replay attacks, generative spoofing, feature imitation, receiver-side manipulation, and adaptive adversaries, with recent OSNMA replay and open-source signal-generation studies providing useful test cases [129], [130]. A particularly important direction is to bind RF fingerprinting with cryptographic authentication. The receiver should verify both message legitimacy and physical-source consistency, thereby reducing the risk that a valid message or replayed waveform is accepted from the wrong transmitter [106], [107].

#### *C. Illegal Terminal Detection and Localization: From RF Monitoring to Evidence-Driven Enforcement*

Illegal terminal detection is difficult because unauthorized terminals may be mobile, intermittent, low-power, directional, and located in complex terrain [42], [49]. A single monitoring station may not capture enough evidence for reliable localization. Moreover, the security objective is not merely to detect a signal but to identify whether it corresponds to unauthorized satellite access and to support operational enforcement [136].

Future illegal-terminal work should fuse SATCOM measurement, terminal security, rogue-device identification, and regulatory-grade cybersecurity evidence. Future research should develop evidence-driven terminal detection frameworks that combine spectrum sensing, protocol recognition, access logs, beam footprints, geolocation databases, and multi-station measurements. Privacy and infrastructure-security studies on satellite broadband show why passive interception, terminal exposure, and weak ground/terminal interfaces should be treated as operational evidence sources rather than isolated incidents [139], [140]. Localization should fuse TDOA, FDOA, AOA, received power, polarization, and beam-domain constraints when available. Machine learning can help recognize terminal behavior patterns, but models must be robust to camouflage and sparse observations. Another important issue is the feedback loop between detection and response. Once a suspicious terminal is identified, the system should decide whether to request re-authentication, restrict access, collect additional measurements, switch beams, or coordinate with ground response teams. Thus, illegal terminal defense should be treated as a closed-loop security process rather than a passive sensing problem [134], [142].

#### *D. Space Secure Routing: From Shortest Path to Trustworthy Dynamic Path Selection*

Routing in LEO networks is often studied as a performance optimization problem [148]. However, security changes the

objective. The shortest path may traverse a compromised satellite, a jammed region, or a gateway under attack. The most reliable path may not be the lowest-delay path. Therefore, the open problem is to design routing mechanisms that jointly consider trust, threat, topology dynamics, mission priority, and resource constraints [72], [73].

Future secure routing should combine 3GPP architecture constraints, contact-graph routing, DTN principles, and secure-routing/anomaly-detection studies. Future secure routing should support authenticated link-state dissemination, trust-aware neighbor evaluation, attack-aware path computation, and autonomous route recovery [113], [114]. Recent LEO-access, handover, and resource-allocation surveys show that routing security cannot be separated from user access, beam switching, and time-varying resource scheduling. It should also exploit the predictability of orbital topology defensively. Since future contacts can be predicted, routing protocols can proactively avoid high-risk regions, prepare backup paths, and schedule route changes before attacks cause service interruption [7], [8]. A deeper research question is how to quantify route security. Candidate metrics include compromised-node probability, RF interference risk, gateway trust level, route diversity, service priority, and expected recovery time. These metrics should be combined without making routing computation too heavy for onboard processors [20], [21].

#### *E. Large-Scale Resilient Network Construction: From Redundancy to Mission-Aware Self-Healing*

Large-scale constellations naturally provide some redundancy, but redundancy alone does not guarantee resilience [77], [147]. If routing, gateways, resources, or service orchestration depend on a small set of temporary bottlenecks, a limited attack may still cause large service impact. The open challenge is to construct mission-aware self-healing networks that can predict, absorb, recover from, and adapt to attacks and failures [180].

Future resilience research should integrate 3GPP system/security architecture, LEO network design, and cyber-resilience engineering. Future research should study time-varying resilience. Latency and topology studies of LEO networks show that network centrality, gateway dependence, and path availability vary over time, which makes static resilience assessment insufficient [148]. The importance of a satellite or link changes with orbital position, traffic demand, gateway visibility, and mission schedule. Resilience metrics should therefore be dynamic rather than static. Self-healing should include topology reconstruction, route repair, service migration, resource reallocation, and attack isolation [5], [9]. Mission-aware recovery is also essential: emergency communication, command and control, and safety-critical services should receive higher priority than ordinary traffic during degradation. Another promising direction is cascading-failure modeling. Researchers should determine how local physical, RF, or cyber events propagate through network topology and service dependencies, and how early intervention can prevent system-wide collapse [37], [39].

#### *F. Onboard System Security: From Secure Boot to Full-Lifecycle Trustworthiness*

Secure boot is necessary but insufficient for satellites with long lifecycles and reconfigurable payloads; space-system cybersecurity work stresses that onboard trust must cover hardware, firmware, software, operations, and update mechanisms [44], [45]. The challenge is to maintain trustworthiness from manufacturing to in-orbit operation and decommissioning. Vulnerabilities may originate from supply chains, firmware, operating systems, payload software, update channels, or ground control interfaces [85], [86]. Once launched, remediation is difficult, and a failed update may endanger the mission.

Future onboard security should combine CCSDS secure space-data-system protocols, NIST trustworthy-system engineering, and space cybersecurity lifecycle studies [76], [87]. Future onboard system security should combine hardware root of trust, secure boot, trusted operating systems, authenticated updates, rollback protection, fault-tolerant recovery, and supply-chain verification, with NIST trustworthy-system engineering guidance and space-system minimum requirements serving as useful engineering baselines. Radiation effects should be jointly considered with cyber attacks because both may cause abnormal software behavior. The system must distinguish random faults from malicious modification while avoiding excessive false alarms [19], [77]. A key research direction is secure remote repair. Satellites need the ability to patch vulnerabilities and recover from corrupted software, but update mechanisms are themselves attractive attack targets. Therefore, update design should include strong authentication, version control, staged deployment, dual-image fallback, and operational safety constraints [111].

#### *G. Onboard Trusted Storage and Computing: From Data Integrity to Verifiable Services*

Onboard trusted storage and computing should guarantee not only that data are stored securely but also that service outputs are trustworthy [87], [89]. As satellites perform more onboard processing, data caching, AI inference, and autonomous decisions, the correctness of computation becomes as important as link availability. A satellite that communicates normally but returns forged computation results can still compromise the mission [45], [85].

Future trusted computing should align data integrity, attestation, key management, and auditability with space-data-system security standards. Future research should develop lightweight trusted execution and verification mechanisms suitable for onboard constraints [76], [86]. NIST trustworthy-system engineering and space-data-security architecture guidance provide a useful baseline for designing verifiable, auditable, and lifecycle-aware onboard services. Remote attestation can help ground stations or peer satellites verify software state, but frequent attestation may consume bandwidth and computation. Verifiable computing can prove computation correctness, but general-purpose schemes may be too heavy [74], [77]. Therefore, mission-specific verification is a promising path: critical

computations such as routing decisions, access-control decisions, model inference, and integrity checks may be selectively verified with tailored protocols. Trusted storage should also address freshness and rollback protection, because replaying old but valid data can be as harmful as direct tampering [44], [75].

#### *H. Satellite Quantum Key Distribution: From Demonstration Links to Operational Key Services*

Satellite QKD has demonstrated the feasibility of long-distance quantum-secure key distribution, but operational Satellite Internet requires more than point-to-point demonstrations [185], [186]. The BB84 and entanglement-based protocols define the cryptographic foundation, while practical security analyses and reviews clarify implementation assumptions and side-channel limits. Physical-layer security and wireless key-generation surveys also provide useful context for deciding when channel-derived keys, QKD keys, and conventional key management should complement each other. The open challenge is to transform QKD capability into a managed key service that can support real network operations [187], [188]. This includes scheduling QKD sessions, storing and refreshing keys, distributing keys to applications, integrating with classical authentication, and handling periods when QKD links are unavailable.

Future QKD deployment should bridge theoretical protocols, practical security, satellite demonstrations, and quantum-safe migration. Future research should clarify where satellite QKD provides the highest value [189], [190]. Recent surveys on space quantum communications highlight the engineering constraints of pointing, weather, pass duration, trusted relays, and key management in networked deployment. It may be most suitable for backbone links, strategic ground stations, command networks, and high-security services rather than all user traffic. Hybrid architectures are also important. QKD can be combined with conventional symmetric encryption, public-key authentication, and post-quantum algorithms. Post-quantum cryptography reports and standardization documents show why QKD should be treated as one part of a broader quantum-safe migration strategy [191], [192]. Operational constraints such as weather, optical pointing, satellite pass duration, trusted relays, and key-rate fluctuation should be incorporated into network planning. The security question is not simply whether quantum keys are secure, but whether the entire key lifecycle is secure and available under realistic satellite operations. This operational view is also motivated by the algorithmic threat model behind quantum-safe migration, including factoring and search speedups, and by experimental foundations for entanglement-based links [193], [194].

#### *I. Satellite Internet AI Security: From Model Robustness to Trustworthy Autonomous Operation*

AI security in Satellite Internet should be studied in relation to the specific functions AI performs [82], [83]. Adversarial-learning studies show that perturbation, black-box, poisoning, and backdoor attacks have different assumptions and therefore should not be cited or evaluated as a single generic threat.

Models used for spectrum sensing, illegal terminal detection, routing, collision warning, resource scheduling, and anomaly detection have different risk profiles. A wrong decision in routing may cause service degradation; a wrong decision in collision avoidance or command execution may have physical consequences [84], [178]. Therefore, the open challenge is not generic AI security but trustworthy autonomous operation under satellite constraints.

Future AI-security work should address poisoning, backdoors, robust training, and the coupling between learned decisions and NTN/satellite control loops. Future research should build secure AI lifecycles for satellite applications [35], [177]. Federated-learning backdoor work is relevant when models are trained or updated from distributed operational data, while NTN and software-defined satellite studies identify the control-loop locations where learned decisions may affect handover, routing, and resource allocation. Training data should be traceable and checked for poisoning. Models should be signed, versioned, audited, and stored securely. Inference should be robust to adversarial inputs and should produce confidence estimates [12], [79]. For safety-critical decisions, AI outputs should be constrained by physical rules, security policies, and human-overridable mechanisms. Explainability is particularly important because operators must understand why a model raises an alert, blocks a terminal, changes a route, or recommends a maneuver. Lightweight robust AI is another key direction because onboard deployment cannot assume abundant computation [81], [169].

#### *J. Cross-Space Collaborative Threat Perception and Defense: From Fragmented Alerts to Attack-Chain Reasoning*

The central unresolved problem in Satellite Internet security is cross-space correlation [116], [117]. Physical monitoring, RF sensing, network intrusion detection, onboard logs, and service monitoring may each produce alerts. If these alerts remain fragmented, defenders may miss the attack chain [118], [119]. Conversely, over-correlating unrelated events may produce false alarms and unnecessary service disruption.

Future cross-space defense should combine attack-graph reasoning, satellite incident analysis, counterspace assessment, and system-level cyber-resilience. Future research should develop attack-chain reasoning models that connect observations across spaces [46]. This requirement follows from reported satellite incidents and counterspace analyses where the entry vector, affected asset, and final mission impact often belong to different spaces. A useful model should represent assets, vulnerabilities, events, dependencies, attack actions, uncertainty, and defense options. It should support incremental reasoning as new evidence arrives. For example, RF spoofing evidence, abnormal access attempts, routing degradation, and service anomalies should be fused into a hypothesis about an electromagnetic-to-network-to-service attack [43], [50]. The system should then recommend coordinated actions such as signal re-authentication, terminal isolation, route switching, service migration, and forensic data collection. To be deployable, cross-space defense must also define measurable metrics, including detection time, propagation risk reduction, response

coordination delay, false correlation rate, and mission impact reduction [51], [77].

## VIII. CONCLUSION

Satellite Internet is becoming a foundational infrastructure for global connectivity, 6G networks, emergency communication, national security, and future intelligent services, as reflected by NTN standardization, New Space satellite-communication surveys, and recent satellite-Internet security requirements studies [1], [4], [14]. However, its unique characteristics, including global access openness, electromagnetic exposure, bidirectional mobility, adversarial coexistence in space, predictable topology, and difficult in-orbit maintenance, create a security landscape that differs fundamentally from terrestrial networks.

This article surveyed Satellite Internet security from a four-space perspective, covering physical entity space, electromagnetic signal space, network information space, and system service space. We showed that Satellite Internet threats are not isolated within individual spaces. Instead, attacks may propagate across spaces and form complex attack chains, such as electromagnetic-to-network, electromagnetic-to-physical, network-to-physical, network-to-service, and physical-to-network attacks. To defend against these threats, Satellite Internet security should evolve toward space-ground integrated, cross-space collaborative, intelligence-driven, quantum-safe, and resilient architectures.

Future research should deepen the ten key technologies identified in this survey: space situational awareness, RF-fingerprinting-enabled signal authenticity authentication, illegal terminal detection and localization, space secure routing, large-scale resilient networking, onboard system security, onboard trusted storage and computing, satellite quantum key distribution, Satellite Internet AI security, and cross-space collaborative threat perception and defense. Building secure Satellite Internet requires not only individual defense mechanisms but also a systematic security framework that integrates physical, electromagnetic, network, and service dimensions.

## REFERENCES

- [1] J. Krause, "Non-terrestrial networks (ntn)," 3GPP, 2025, accessed: Jul. 4, 2025. [Online]. Available: <https://www.3gpp.org/technologies/ntn-overview>.
- [2] 3GPP, "Release 17," 3GPP, 2022, accessed: Jun. 23, 2026. [Online]. Available: <https://www.3gpp.org/specifications-technologies/releases/release-17>.
- [3] X. Lin, S. Rommer, S. Euler, E. A. Yavuz, and R. S. Karlsson, "5G from space: An overview of 3GPP non-terrestrial networks," *IEEE Commun. Stand. Mag.*, vol. 5, no. 4, pp. 147–153, 2021.
- [4] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff *et al.*, "Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 70–109, 2020.
- [5] C. Westphal, L. Han, and R. Li, "LEO satellite networking relaunched: Survey and current research challenges," Oct. 2023, arXiv:2310.07646.
- [6] I. Del Portillo, B. G. Cameron, and E. F. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronaut.*, vol. 159, pp. 123–135, 2019.
- [7] X. Qi, J. Ma, D. Wu, L. Liu, and S. Hu, "A survey of routing techniques for satellite networks," *J. Commun. Inf. Netw.*, vol. 1, no. 4, pp. 66–85, 2016.

- [8] E. A. Elbehiry, H. A. TagEldien, A. Fares, and B. M. ElHalawany, "Survey on routing algorithms for LEO constellations network," *Fayoum Univ. J. Eng.*, vol. 7, no. 2, pp. 89–99, 2024.
- [9] M. Handley, "Delay is not an option: Low latency routing in space," in *Proc. 17th ACM Workshop Hot Topics Netw.*, 2018, pp. 85–91.
- [10] M. Á. Vázquez, A. Perez-Neira, D. Christopoulos, S. Chatzinotas, B. Ottersten, P.-D. Arapoglou, A. Ginesi, and G. Taricco, "Precoding in multibeam satellite communications: Present and future challenges," *IEEE Wireless Commun.*, vol. 23, no. 6, pp. 88–95, 2016.
- [11] A. Guidotti, A. Vanelli-Coralli, M. Conti, S. Andrenacci, S. Chatzinotas, N. Maturo, B. Evans, A. Awoseyila, A. Ugolini, and T. e. a. Foggi, "Architectures and key technical challenges for 5G systems incorporating satellites," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2624–2639, 2019.
- [12] W. Jiang, "Software defined satellite networks: A survey," *Digit. Commun. Netw.*, vol. 9, no. 6, pp. 1243–1264, 2023.
- [13] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," *Sensors*, vol. 24, no. 9, p. 2897, 2024.
- [14] Y. Zhang, S. Zhao, J. He, Z. Zhang, and et al., "Satellite internet security: Requirement, current status and trends," *J. Cyberspace Secur. Sci.*, vol. 8, no. 2, p. 4, 2024.
- [15] H. N. Nguyen, S. Lepaja, J. Schuringa, and H. R. Van As, "Handover management in low earth orbit satellite ip networks," in *Proc. IEEE GLOBECOM*, 2001, pp. 2730–2734.
- [16] D. A. Vallado, *Fundamentals of Astrodynamics and Applications*. Springer, 2001, vol. 12.
- [17] D. Bhattacharjee and A. Singla, "Network topology design at 27,000 km/hour," in *Proc. 15th Int. Conf. Emerging Netw. Exp. Technol.*, 2019, pp. 341–354.
- [18] M. Scholl and T. Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations*. NIST, 2023.
- [19] G. Falco, N. Boschetti, A. Viswanathan, B. Bailey, C. Maple, G. K. Kurt, and et al., "Minimum requirements for space system cybersecurity—ensuring cyber access to space," in *Proc. IEEE 10th Int. Conf. Space Mission Challenges Inf. Technol.*, 2024, pp. 78–88.
- [20] Y. Yan, G. Han, and H. Xu, "A survey on secure routing protocols for satellite network," *J. Netw. Comput. Appl.*, vol. 145, p. 102415, 2019.
- [21] M. Zhuo, L. Liu, S. Zhou, and Z. Tian, "Survey on security issues of routing and anomaly detection for space information networks," *Scientific Reports*, vol. 11, no. 1, p. 22261, 2021.
- [22] C. Jiang, X. Wang, J. Wang, H.-H. Chen, and Y. Ren, "Security in space information networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 82–88, 2015.
- [23] M. Strohmeier, D. Moser, M. Schafer, V. Lenders, and I. Martinovic, "On the applicability of satellite-based air traffic control communication for security," *IEEE Commun. Mag.*, vol. 57, no. 9, pp. 79–85, 2019.
- [24] J. Wang, Y. Zhang, S. Zhao, J. He, Y. Shen, and X. Jiang, "A survey on authentication in satellite internet," *J. Netw. Netw. Appl.*, vol. 2, no. 4, pp. 183–194, 2022.
- [25] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, 2021.
- [26] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, and et al., "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1604–1652, 2023.
- [27] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Comput. Netw.*, vol. 216, p. 109246, 2022.
- [28] Y. Zhang, S. Zhao, J. He, Y. Zhang, Y. Shen, and X. Jiang, "A survey of secure communications for satellite internet based on cryptography and physical layer security," *IET Inf. Secur.*, vol. 2023, no. 1, p. 5604802, 2023.
- [29] Y. Meng, C. Ke, and Z. Huang, "Comprehensive survey towards security authentication methods for satellite communication systems," Mar. 2025, arXiv:2503.23277.
- [30] J. Wang and X. Zhao, "A review of key technologies and research progress of satellite internet communication security," in *Proc. 2026 9th Int. Conf. Adv. Algorithms Control Eng.*, 2026, pp. 1–9.
- [31] M. Werner, "A dynamic routing concept for ATM-based satellite personal communication networks," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 8, pp. 1636–1648, 1997.
- [32] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," *IEEE network*, vol. 35, no. 2, pp. 244–251, 2020.
- [33] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, 2020.
- [34] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, p. 110301, 2021.
- [35] G. Geraci, D. López-Pérez, M. Benzaghta, and S. Chatzinotas, "Integrating terrestrial and non-terrestrial networks: 3D opportunities and challenges," *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 42–48, 2022.
- [36] D. Bhattacharjee, W. Aqeel, I. N. Bozkurt, A. Aguirre, B. Chandrasekaran, P. B. Godfrey, and et al., "Gearing up for the 21st century space race," in *Proc. 17th ACM Workshop Hot Topics Netw.*, 2018, pp. 113–119.
- [37] D. Vasisht, J. Shenoy, and R. Chandra, "L2D2: Low latency distributed downlink for LEO satellites," in *Proc. ACM SIGCOMM*, 2021, pp. 151–164.
- [38] G. Giuliani, T. Klenze, M. Legner, D. Basin, A. Perrig, and A. Singla, "Internet backbones in space," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 50, no. 1, pp. 25–37, 2020.
- [39] T. Klenze, G. Giuliani, C. Pappas, A. Perrig, and D. Basin, "Networking in heaven as on earth," in *Proc. 17th ACM Workshop Hot Topics Netw.*, 2018, pp. 22–28.
- [40] J. Zhang, L. Yang, Q. Wu, G. Pan, L. Xu, D. Niyato, and M.-S. Alouini, "Resource allocation and management in multi-satellite collaborative networks: Frameworks, key techniques and challenges," *IEEE Aerosp. Electron. Syst. Mag.*, 2026.
- [41] E. Papapetrou, S. Karapantazis, G. Dimitriadis, and F.-N. Pavlidou, "Satellite handover techniques for LEO networks," *Int. J. Satell. Commun. Netw.*, vol. 22, no. 2, pp. 231–245, 2004.
- [42] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw.*, 2019, pp. 277–284.
- [43] J. Pavur and I. Martinovic, "SoK: Building a launchpad for impactful satellite cyber-security research," Oct. 2020, arXiv:2010.10872.
- [44] CCSDS, "The application of CCSDS protocols to secure systems," CCSDS, Green Book CCSDS 350.0-G-2, Jan. 2006.
- [45] I. A. Sanchez, G. Moury, C. Biggerstaff, B. Saba, D. Fischer, and H. Weiss, "Towards completion of the CCSDS space data link security protocol," in *Proc. IEEE Aerosp. Conf.*, 2012, pp. 1–18.
- [46] J. A. Guerrero-Saade and M. Van Amerongen, "Acidrain— a modem wiper rains down on europe," *Sentinel Labs*, vol. 31, 2022.
- [47] J. Slowik, "Reviewing the 2022 Ka-Sat incident & implications for distributed communication environments," *Virus Bulletin*, pp. 7–8, 2024.
- [48] L. Wouters, S. Trickle, D. Kennedy, and B. Ragsdale, "Glitched on earth by humans: a black-box security evaluation of the SpaceX starlink user terminal," *DEF CON*, 2022.
- [49] R. Santamarta, "SATCOM terminals: Hacking by air, sea, and land," *DEFCON White Paper*, 2014.
- [50] T. Harrison, K. Johnson, J. Moye, M. Young et al., *Space threat assessment 2020*. CSIS, 2022.
- [51] B. Weeden and V. Samson, "Global counterspace capabilities: An open source assessment," Secure World Foundation, Tech. Rep., 2018.
- [52] Cybersecurity and Infrastructure Security Agency, "Russian state-sponsored and criminal cyber threats to critical infrastructure," CISA, Tech. Rep., Apr. 2022.
- [53] A. Mohammed, "Cybersecurity for space systems: Securing satellites and communications against threats," *Innov. Comput. Sci. J.*, pp. 1–7, 2024.
- [54] S. Le May, S. Gehly, B. Carter, and S. Flegel, "Space debris collision probability analysis for proposed global broadband constellations," *Acta Astronaut.*, vol. 151, pp. 445–455, 2018.
- [55] A. Rossi, A. Petit, and D. McKnight, "Short-term space safety analysis of LEO constellations and clusters," *Acta Astronaut.*, vol. 175, pp. 476–483, 2020.
- [56] A. Mohammed, "Protecting space assets: Cybersecurity challenges and solutions for the final frontier," *Balt. J. Eng. Technol.*, vol. 2, no. 1, pp. 55–61, 2023.
- [57] G. Falco, "Job one for space force: Space asset cybersecurity," Belfer Center for Science and International Affairs, Harvard Kennedy School, Tech. Rep. Cyber Security Project Paper, Jul. 2018.
- [58] —, "Cybersecurity principles for space systems," *J. Aerosp. Inf. Syst.*, vol. 16, no. 2, pp. 61–70, 2019.

- [59] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meet. Satell. Div. Inst. Navig.*, 2008, pp. 2314–2325.
- [60] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, 2011, pp. 75–86.
- [61] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *J. Secur. Adm.*, vol. 25, no. 2, pp. 19–27, 2002.
- [62] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proc. 2010 Int. Tech. Meet. Inst. Navig.*, 2010, pp. 698–712.
- [63] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.
- [64] A. Jafarinia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of anti-spoofing techniques," *Int. J. Navig. Obs.*, vol. 2012, no. 1, p. 127072, 2012.
- [65] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 1–31, 2016.
- [66] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, 2016.
- [67] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the 2009 international technical meeting of the institute of navigation*, 2009, pp. 124–130.
- [68] L. Wood, A. Clerget, I. Andrikopoulos, G. Pavlou, and W. Dabbous, "IP routing issues in satellite constellation networks," *Int. J. Satell. Commun.*, vol. 19, no. 1, pp. 69–92, 2001.
- [69] T. Henderson and R. Katz, "Network simulation for LEO satellite networks," in *Proc. 18th Int. Commun. Satell. Syst. Conf. Exhib.*, 2000, p. 1237.
- [70] COSIC, KU Leuven, "Lennert wouters reveals one of the first security breakdowns of starlink's user terminals," COSIC, KU Leuven, Aug. 2022, accessed: Jun. 23, 2026. [Online]. Available: <https://www.esat.kuleuven.be/cosic/news/lennert-wouters-reveals-one-of-the-first-security-breakdowns-of-starlinks-user-terminals/>.
- [71] E. Ekici, I. F. Akyildiz, and M. D. Bender, "A distributed routing algorithm for datagram traffic in LEO satellite networks," *IEEE/ACM Trans. Netw.*, vol. 9, no. 2, pp. 137–147, 2002.
- [72] J. A. Fraire, O. De Jonckère, and S. C. Burleigh, "Routing in the space internet: A contact graph routing tutorial," *J. Netw. Comput. Appl.*, vol. 174, p. 102884, 2021.
- [73] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, and *et al.*, "Delay-tolerant networking: An approach to interplanetary internet," *IEEE Commun. Mag.*, vol. 41, no. 6, pp. 128–136, 2003.
- [74] National Institute of Standards and Technology, "Security and privacy controls for information systems and organizations," NIST, Special Publication NIST SP 800-53 Rev. 5, Dec. 2020.
- [75] Joint Task Force, "Risk management framework for information systems and organizations: A systems life cycle approach for security and privacy," NIST, Special Publication NIST SP 800-37 Rev. 2, Dec. 2018.
- [76] National Institute of Standards and Technology, "Engineering trustworthy secure systems," NIST, Special Publication NIST SP 800-160 Vol. 1 Rev. 1, 2025.
- [77] —, "Developing cyber-resilient systems: A systems security engineering approach," NIST, Special Publication NIST SP 800-160 Vol. 2 Rev. 1, 2025.
- [78] Y. Zhang, Y. Wang, Y. Hu, Z. Lin, Y. Zhai, L. Wang, Q. Zhao, K. Wen, and L. Kang, "Security performance analysis of LEO satellite constellation networks under DDoS attack," *Sensors*, vol. 22, no. 19, p. 7286, 2022.
- [79] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," Dec. 2014, arXiv:1412.6572.
- [80] T. Gu, B. Dolan-Gavitt, and S. Garg, "Badnets: Identifying vulnerabilities in the machine learning model supply chain," Aug. 2017, arXiv:1708.06733.
- [81] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *Proc. 2017 ACM Asia Conf. Comput. Commun. Secur.*, 2017, pp. 506–519.
- [82] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," Jun. 2012, arXiv:1206.6389.
- [83] X. Chen, C. Liu, B. Li, K. Lu, and D. Song, "Targeted backdoor attacks on deep learning systems using data poisoning," Dec. 2017, arXiv:1712.05526.
- [84] Y. Liu, S. Ma, Y. Aafer, W.-C. Lee, J. Zhai, W. Wang, and *et al.*, "Trojaning attack on neural networks," in *Proc. NDSS 2018*, 2018.
- [85] I. A. Sanchez, G. Moury, and H. Weiss, "The CCSDS space data link security protocol," in *Proc. MILCOM 2010*, 2010, pp. 219–224.
- [86] CCSDS, "Space data link security protocol—extended procedures—summary of concept and rationale," CCSDS, Green Book CCSDS 350.11-G-1, Jul. 2024.
- [87] —, "Ccsds cryptographic algorithms," CCSDS, Blue Book CCSDS 352.0-B-1, Nov. 2012.
- [88] ITU-T, "Security architecture for systems providing end-to-end communications," ITU-T, Recommendation ITU-T X.805, Oct. 2003.
- [89] E. Barker and Q. Dang, "Recommendation for key management: Part 1 – general," National Institute of Standards and Technology, Special Publication NIST SP 800-57 Part 1 Rev. 5, May 2020.
- [90] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.
- [91] H. Wang, Y. Zhang, X. Zhu, J. He, S. Zhao, Y. Shen, and X. Jiang, "Practical spoofing attacks on Galileo open service navigation message authentication," Jan. 2025, arXiv:2501.09246.
- [92] H. Wang, Y. Zhang, Y. Shen, J. Zhu, Y. Chen, and X. Jiang, "Novel replay attacks against Galileo open service navigation message authentication," in *Proc. ION GNSS+ 2023*, 2023, pp. 3897–3907.
- [93] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service," in *Proc. ION GNSS+ 2014*, 2014, pp. 2810–2827.
- [94] G. Maruccio, M. Ligios, S. A. Chala, and P. Rosengren, "Galileo open service navigation message authentication: Exploitation in the frame of an E-Security infrastructure," in *Proc. ENC 2020*, 2020, pp. 1–10.
- [95] M. Nicola, B. Motella, M. Pini, and E. Falletti, "Galileo OSNMA public observation phase: Signal testing and validation," *IEEE Access*, vol. 10, pp. 27960–27969, 2022.
- [96] X. Chen, R. Luo, T. Liu, H. Yuan, and H. Wu, "Satellite navigation signal authentication in GNSS: A survey on technology evolution, status, and perspective for BDS," *Remote Sens.*, vol. 15, no. 5, p. 1462, 2023.
- [97] European Union Agency for the Space Programme, "Galileo open service navigation message authentication adds another layer of protection against gnss interference," EUSPA, Jul. 2025, accessed: Jun. 23, 2026. [Online]. Available: <https://www.euspa.europa.eu/newsroom-events/news/galileo-open-service-navigation-message-authentication-adds-another-layer>.
- [98] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navig. J. Inst. Navig.*, vol. 59, no. 3, pp. 177–193, 2012.
- [99] K. Wesson and T. Humphreys, "Hacking drones," *Sci. Am.*, vol. 309, no. 5, pp. 54–59, 2013.
- [100] G. Seco-Granados, D. Gómez-Casco, J. A. López-Salcedo, and I. Fernández-Hernández, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *GPS Solut.*, vol. 25, no. 2, p. 33, 2021.
- [101] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, 2017.
- [102] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navig. J. Inst. Navig.*, vol. 64, no. 1, pp. 51–66, 2017.
- [103] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the galileo open service," *Navig. J. Inst. Navig.*, vol. 63, no. 1, pp. 85–102, 2016.
- [104] H. Wang, Y. Zhang, X. Zhu, J. He, S. Zhao, and Y. Shen, "OSNMA-SDR-SIM: An open-source tool for generating OSNMA-enabled Galileo satellite signal," in *Proc. ION GNSS+ 2025*, Sep. 2025, pp. 3184–3192.
- [105] J. Wang, Y. Zhang, X. Zhu, J. He, S. Zhao, Y. Shen, and X. Jiang, "GCI-GANomaly: A novel GPS spoofing detection scheme based on grayscale constellation image," *IEEE Trans. Inf. Forensics Secur.*, vol. 21, pp. 3022–3037, 2026.
- [106] H. Wang, S. Guo, Z. Liu, Y. Zhang, Y. Shen, and X. Jiang, "GNSS signal spoofing detection based on satellite oscillator stability," in *Proc. SAT-NET 2024*. Los Alamitos, CA, USA: IEEE Computer Society, Oct. 2024, pp. 44–51.

- [107] Y. Zhang, J.-N. Wang, Z. Zheng, Y. Shen, Y. Jiang, and M. Yang, "Variational AutoEncoder-based radio frequency fingerprinting for GPS anti-spoofing," in *Proc. NaNA 2024*, 2024, pp. 172–178.
- [108] A. Budiyo, "Principles of GNSS, inertial, and multi-sensor integrated navigation systems," *Ind. Robot Int. J.*, no. 3, 2012.
- [109] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, Tech. Rep., Jan. 2012.
- [110] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, 2016.
- [111] NASA Office of Inspector General, "NASA's Efforts to Identify Near-Earth Objects and Mitigate Hazards," National Aeronautics and Space Administration, Tech. Rep. IG-14-030, Sep. 2014.
- [112] Q. Zhu, X. Wang, H. Yang, and Y. Cao, "Design and evaluation of dynamic topology for mega constellation networks," *Electronics*, vol. 12, no. 8, p. 1784, 2023.
- [113] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-tolerant networking architecture," IRTF, Informational RFC 4838, Apr. 2007.
- [114] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc. ACM SIGCOMM 2003*, 2003, pp. 27–34.
- [115] X. Chen, Z. Ji, S. Wu, H. Jia, A. Xiao, and C. Jiang, "A distributed routing algorithm for LEO satellite networks: A multiagent transformer-MIX learning approach," *IEEE Internet Things J.*, vol. 12, no. 11, pp. 15748–15763, 2025.
- [116] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proc. IEEE Symp. Secur. Priv.*, 2002, pp. 273–284.
- [117] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: A logic-based network security analyzer," in *Proc. USENIX Secur. Symp.*, 2005, pp. 113–128.
- [118] X. Ou, W. F. Boyer, and M. A. McQueen, "A scalable approach to attack graph generation," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 336–345.
- [119] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 61–74, 2011.
- [120] J. Zhang, Y. Cai, C. Xue, Z. Xue, and H. Cai, "LEO mega constellations: Review of development, impact, surveillance, and governance," *Space Sci. Technol.*, vol. 2, p. 9865174, May 2022.
- [121] F. Massimi, P. Ferrara, and F. Benedetto, "Deep learning methods for space situational awareness in mega-constellations satellite-based Internet of Things networks," *Sensors*, vol. 23, no. 1, p. 124, 2022.
- [122] Q. Jia, J. Xiao, L. Bai, Y. Zhang, R. Zhang, and M. Feroskhan, "Space situational awareness systems: Bridging traditional methods and artificial intelligence," *Acta Astronaut.*, vol. 228, pp. 321–330, 2025.
- [123] P. Yue, J. An, J. Zhang, G. Pan, S. Wang, P. Xiao, and et al., "On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends," arXiv, Jan. 2022, arXiv:2201.03063.
- [124] J. Pavur and I. Martinovic, "Building a launchpad for satellite cybersecurity research: lessons from 60 years of spaceflight," *J. Cybersecurity*, vol. 8, no. 1, p. tyac008, 2022.
- [125] S. Zhu, Y. Zhang, J. Zhu, Y. Chen, Y. Shen, and X. Jiang, "3D convolution-based radio frequency fingerprinting for satellite authentication," in *Proc. IEEE GLOBECOM 2023*, 2023, pp. 7586–7591.
- [126] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges," *Comput. Netw.*, vol. 219, p. 109455, 2022.
- [127] J. Zhang, F. Ardizzone, M. Piana, G. Shen, and S. Tomasin, "Physical layer-based device fingerprinting for wireless security: From theory to practice," *IEEE Trans. Inf. Forensics Secur.*, vol. 20, pp. 5296–5325, May 2025.
- [128] K. Merchant, S. Revay, G. Stantchev, and B. Noursain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Top. Signal Process.*, vol. 12, no. 1, pp. 160–167, 2018.
- [129] W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth, and E. S. Lohan, "A survey of spoofer detection techniques via radio frequency fingerprinting with focus on the GNSS pre-correlation sampled data," *Sensors*, vol. 21, no. 9, p. 3012, 2021.
- [130] F. Gallardo, A. Pérez-Yuste, and A. Kononov, "Satellite fingerprinting methods for GNSS spoofing detection," *Sensors*, vol. 24, no. 23, p. 7698, 2024.
- [131] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4829–4842, 2018.
- [132] F. Restuccia, S. D'Oro, A. Al-Shawabka, M. Belgiovine, L. Angioloni, S. Ioannidis, K. Chowdhury, and T. Melodia, "DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms," in *Proc. ACM MobiHoc 2019*, 2019, pp. 51–60.
- [133] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1761–1789, 2017.
- [134] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 2015.
- [135] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, "RF fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15518–15531, 2020.
- [136] M. Barbeau, J. Hall, and E. Kranakis, "Detection of rogue devices in bluetooth networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Int. Conf. Commun. Comput. Netw.*, 2006, pp. 4–6.
- [137] C. Hao, D. Feng, Q. Zhang, and X.-G. Xia, "Interference geolocation in satellite communications systems: An overview," *IEEE Veh. Technol. Mag.*, vol. 16, no. 1, pp. 66–74, 2020.
- [138] S. Wang and W. Wang, "A review of satellite passive localization: Principles, parameter estimation, and positioning algorithms," *J. Netw. Netw. Appl.*, vol. 5, no. 3, pp. 110–119, 2025.
- [139] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 6, pp. 1180–1192, 2015.
- [140] A. C. Polak and D. L. Goeckel, "RF fingerprinting of users who actively mask their identities with artificial distortion," in *Proc. 45th Asilomar Conf. Signals Syst. Comput.*, 2011, pp. 270–274.
- [141] H. Jung, J. Kang, and S. Kim, "EKF-Based geolocation using TDOA/FDOA measurements in dual-satellite," in *Proc. ICTC 2022*, Oct. 2022, pp. 1179–1182.
- [142] K. Olga Greuter and D. K. Sarmah, "The baseline of global consumer cyber security standards for IoT: quality evaluation," *J. Cyber Secur. Technol.*, vol. 6, no. 4, pp. 175–200, 2022.
- [143] G. Liu, X. Jiang, H. Li, S. Sun, Z. Zhang, and G. Liang, "An improved DTN scheme for large-scale LEO satellite networks," *Wireless Commun. Mob. Comput.*, vol. 2023, no. 1, p. 4899124, 2023.
- [144] P. Hu, "A cross-layer descent approach for resilient network operations of proliferated LEO satellites," in *Proc. IEEE WCNC 2023*, 2023, pp. 1–6.
- [145] X. Xu, Z. Gao, and A. Liu, "Robustness of satellite constellation networks," *Comput. Commun.*, vol. 210, pp. 130–137, 2023.
- [146] L. Zhang and Y. Du, "Cascading failure model and resilience enhancement scheme of space information networks," *Reliab. Eng. Syst. Saf.*, vol. 237, p. 109379, 2023.
- [147] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5g security in 3GPP," in *Proc. IEEE CSCN 2017*, Sep. 2017, pp. 181–186.
- [148] G. Masini, "A guide to NG-RAN architecture," in *5G and Beyond: Fundamentals and Standards*. Springer, 2021, pp. 233–258.
- [149] O. Haxhiavdyli, A. R. Deepti, D. Canhasi, B. P. Etemi, and D. Samanta, "Cybersecurity in space exploration: Protecting satellites and space missions," in *Proc. Int. Conf. Data Anal. Manag.*, 2025, pp. 11–19.
- [150] H. Li, V. Novruzov, N. Singh, L. Wu, M. Rostami, and A.-R. Sadeghi, "Aegissat: Securing AI-Enabled SoC FPGA satellite platforms," in *Proc. 3S 2025*, 2025, pp. 1–13.
- [151] Y. Huang, X. Zhang, and Z. Xu, "SatEdge: Platform of edge cloud at satellite and scheduling mechanism for microservice modules," *IEEE Access*, vol. 11, pp. 126283–126294, 2023.
- [152] P. Maene, J. Götzfried, R. De Clercq, T. Müller, F. Freiling, and I. Verbauwhede, "Hardware-based trusted computing architectures for isolation and attestation," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 361–374, 2017.
- [153] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 57–64.
- [154] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, 2015.
- [155] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

- [156] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [157] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.
- [158] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.
- [159] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.
- [160] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.
- [161] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [162] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.
- [163] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 146–152, 2018.
- [164] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, "Machine learning for wireless communications in the internet of things: A comprehensive survey," *Ad Hoc Netw.*, vol. 93, p. 101913, 2019.
- [165] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, 2019.
- [166] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE J. Radio Freq. Identif.*, vol. 4, no. 3, pp. 222–233, 2020.
- [167] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," Dec. 2013, arXiv:1312.6199.
- [168] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proc. IEEE Symp. Secur. Priv.*, May 2017, pp. 39–57.
- [169] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," Jun. 2017, arXiv:1706.06083.
- [170] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 2018.
- [171] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 640–660, 2018.
- [172] Z. J. Al-Araji, S. S. S. Ahmed, R. S. Abdullah, A. A. Mutlag, H. A. A. Raheem, and S. R. H. Basri, "Attack graph reachability: Concept, analysis, challenges and issues," *Netw. Secur.*, vol. 2021, no. 6, pp. 13–19, 2021.
- [173] V. P. Kafle, M. Sekiguchi, H. Asaeda, and H. Harai, "Validation of integrated network control architecture for fixed, mobile and satellite convergence," in *Proc. ITU K 2024*, Oct. 2024, pp. 1–8.
- [174] B. Jarvis, "Adoption and use of Internet of Things and the implications for adaptive regulation," Master's thesis, Johannesburg, South Africa, 2024.
- [175] V. P. Kafle, Y. Fukushima, and H. Harai, "Internet of Things standardization in ITU and prospective networking technologies," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 43–49, 2016.
- [176] C. D. Gedara, M. D. Khattak, M. A. Ullah, and K. Mikhaylov, "Direct-to-satellite connectivity for IoT: Overview and potential of reduced capability (RedCap)," in *Proc. IEEE WF-IoT 2023*, Oct. 2023, pp. 1–8.
- [177] M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, and *et al.*, "Evolution of non-terrestrial networks from 5g to 6g: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2633–2672, 2022.
- [178] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How to backdoor federated learning," in *Proc. AISTATS 2020*, Jun. 2020, pp. 2938–2948.
- [179] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Commun. Mob. Comput.*, vol. 2022, no. 1, p. 6476274, 2022.
- [180] F. Launay, *NG-RAN and 5G-NR: 5G Radio Access Network and Radio Interface*. Wiley, 2021.
- [181] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM MobiCom 2008*, 2008, pp. 116–127.
- [182] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 1–29, 2012.
- [183] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2604–2616, 2021.
- [184] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for LoRa," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 774–787, 2022.
- [185] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.
- [186] I. Volovich, "Quantum cryptography in space and Bell's theorem," in *Foundations of Probability and Physics*. World Scientific, 2001, pp. 364–372.
- [187] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.
- [188] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.
- [189] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.
- [190] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, p. 030501, 2018.
- [191] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone *et al.*, "Advances in space quantum communications," *IET Quantum Commun.*, vol. 2, no. 4, pp. 182–217, 2021.
- [192] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, no. 24, pp. 4337–4341, Dec. 1995.
- [193] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.
- [194] W. Jiang, Y. Zhang, H. Han, and J. Mu, "Quantum communication in self-organizing satellite networks: Challenges and opportunities," *IEEE Commun. Stand. Mag.*, vol. 9, no. 3, pp. 15–25, Sep. 2025.