This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2024.3408277

Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments

Sara Salim, Nour Moustafa, and Martin Reisslein

***Abstract*—Satellite communications (Satcoms) systems have become an integral part of modern society, providing critical infrastructure for a wide range of applications. However, as the reliance on Satcoms has increased, cyberattacks on Satcoms systems have emerged as a severe concern, with the potential to cause significant disruption, economic losses, and even loss of life. We first give a tutorial-style overview of the architecture of a Satcoms system, which typically consists of a space segment, a ground segment (encompassing the terrestrial ground stations and users), and the links segment. Following the taxonomy provided by this segment structure, we provide—to the best of our knowledge—the first comprehensive survey of the state-of-the-art cyberattacks (cyberthreats) on all three segments of Satcoms systems. For each Satcoms system segment, we organize the cyberattacks according to categories of Satcoms-specific cyberattacks, which we relate to the threat classifications in the general STRIDE cyberthreat model. Also, for all three segments of Satcoms systems, we comprehensively survey the general cybersecurity strategies and the specific cybersecurity mechanisms (techniques) that defend Satcoms systems against cyberattacks. We distill the critical learned lessons associated with Satcoms cybersecurity strategies, such as the need to balance security with cost-effectiveness. Finally, we outline the open challenges and future research directions in Satcoms systems cybersecurity.**

***Index Terms*—Cyberattack, Cybersecurity, Ground segment, Links segment, Space segment, Satellite communications.**

I. Introduction

Space has always inspired researchers and scientists. Ranging from the natural sciences to engineering, the study of space has provided technological advances and substantially expanded humanity's scientific knowledge [1]. It has also enhanced our daily lives in several ways; according to the European Space Agency (ESA) [2], every Euro invested in the space industry returns six Euros to the community. Till recently, space was affiliated with state funding, since the high up-front costs and enormous challenges made the space industry unattractive to private entities [3]. Nowadays, newly emerging Satellite Communications (Satcoms) systems open up unique future opportunities for space exploration and exploitation [4], [5], [6], [7].

Satcoms systems leverage artificial satellites, encompassing those positioned in Geostationary Orbit (GEO) and Low Earth Orbit (LEO). These satellites receive signals from Earth, amplify them, and transmit them back to terrestrial receivers, facilitating widespread telecommunications [8], [9]. Serving as the linchpin of numerous services and applications [10], [11], Satcoms systems play a pivotal role in diverse areas, ranging from navigation and TV broadcasts to phone networks, electricity grids, weather forecasts, climate monitoring, and military communications [12]. Additionally, Satcoms systems are integral to the burgeoning realm of the Internet of Things (IoT) [13], [14]. A typical Satcoms system, illustrated in Figure 1, comprises three primary segments: space segment, ground segment (including end-users), and links segment. Satellites within the space segment constitute the key components of this structural framework [15].

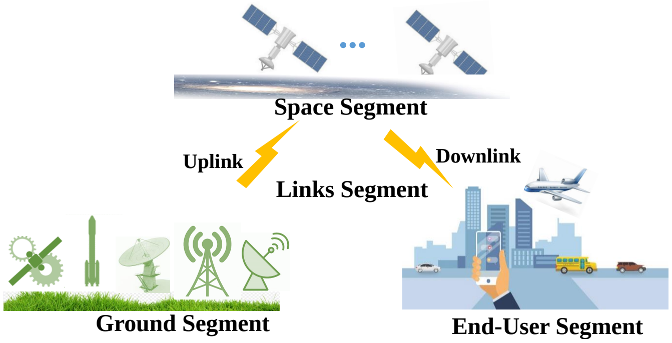


Fig. 1. Illustration of typical Satcoms system segments.

A. Motivation

Recently, Satcoms systems have witnessed a boom in interest, driven by technology advancements and funded by private investments and initiatives [16], [17]. Along with the Internet-based application revolution, Satcoms systems are undergoing a transformation phase that centers the system structure on data services, specifically, broadband Satcoms [6], [7].

This transformation is propelled by two primary drivers. First, there is an urgent need to extend broadband services to underserved regions, including developing nations and airborne applications. The global demand for connectivity has made Satcoms systems critical for bridging the digital divide [19], [20].

Second, there is a growing preference for media streaming that is replacing traditional linear media transmission [6]. Linear media transmission refers to the conventional broadcasting

S. Salim and N. Moustafa are with the University of New South Wales, PO Box 7916, ACT 2612, Canberra, Australia, (e-mail: s.salim@unsw.edu.au, nour.moustafa@unsw.edu.au).

M. Reisslein is with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287-5706 USA (e-mail: reisslein@asu.edu).

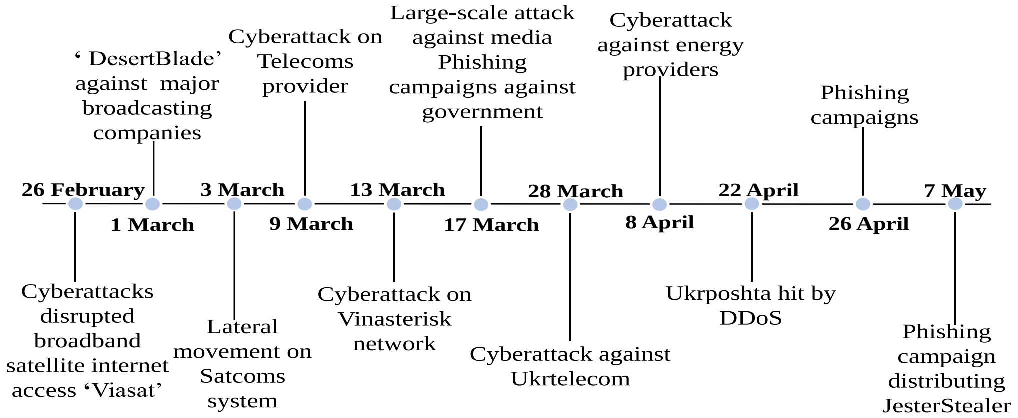

‘ DesertBlade’ against major broadcasting companies
Cyberattack on Telecoms provider
Large-scale attack against media Phishing campaigns against government
Cyberattack against energy providers
Phishing campaigns
26 February
1 March
3 March
9 March
13 March
17 March
28 March
8 April
22 April
26 April
7 May
Cyberattacks disrupted broadband satellite internet access ‘Viasat’
Lateral movement on Satcoms system
Cyberattack on Vinasterisk network
Cyberattack against Ukrtelecom
Ukrposhta hit by DDoS
Phishing campaign distributing JesterStealer

Fig. 2. Timeline of cyberattacks on Ukraine’s Satcoms systems from February to May 2022 [18].

of scheduled television programs, whereas the preference for media streaming signifies a shift towards on-demand and personalized media consumption. This shift in preference for on-demand media streaming has been a significant catalyst for the evolution and expansion of Satcoms systems, as they are instrumental in delivering high-quality, uninterrupted media content to a global audience.

Satcoms systems have evolved into a critical platform for the seamless integration of both wired and wireless technologies, addressing a diverse range of specific use cases [21], [20]. Additionally, private enterprises have broadened their production and launch capabilities, democratizing access to space, a realm once predominantly controlled by governments and large international organizations [22], [19].

This rapid expansion in space activities has led to the proliferation of innovative Satcoms-based broadband and environmental sensing services, necessitating advancements in both Satcoms architecture and, critically, Satcoms cybersecurity [20]. While Satcoms systems play a pivotal role in delivering these services, they also represent a singular point of vulnerability. This vulnerability implies that the failure of Satcoms systems could result in the collapse of numerous critical services [15]. As a consequence, Satcoms systems have become enticing targets for various threat actors, including commercial competitors, cyber adversaries, and the militaries of nation-states [21], [23].

In addition to these challenges, there is a notable absence of comprehensive international governmental oversight concerning cybersecurity requirements for space assets [19], [21]. While some nations may have centralized government oversight within their borders, the international level lacks a robust regulatory authority, i.e., a governing body or organization with significant and effective regulatory and oversight capabilities is lacking. Despite efforts by entities, such as the United Nations, including the United Nations Office of Outer Space Affairs (UNOOSA), their regulatory influence in this domain is relatively limited [20]. This regulatory gap results in a situation where Satcoms systems currently lack universally agreed-upon cybersecurity standards, potentially rendering them susceptible to attacks without clear attribution [12], [15], [21].

Despite being a relatively recent concern, the threat of cyberattacks on Satcoms systems has given rise to substantial concerns about the sustainability of satellite systems [19], [24], [25]. These vulnerabilities, which can endanger the success of various missions, encompass not only launch systems but also communications infrastructure, telemetry, tracking, and command systems [26], [24]. While there are international laws and regulations that apply to space activities, including the peaceful use of outer space, the absence of comprehensive and universally accepted cybersecurity standards has created ambiguities and challenges in enforcing these legal frameworks effectively. Therefore, while there is a legal framework in place, it is not always sufficient to prevent or mitigate cyberattacks on Satcoms systems. Indeed, alarming instances of hostile cyberattacks have disrupted Satcoms systems, flagrantly breaching international law [27], [18], [19].

For instance, Ukraine’s Satcoms systems have been targeted by such cyberattacks. The timeline in Figure 2 illustrates significant cyberattacks, as documented by the CyberPeace Institute [18]. These include five major Satcoms cyberattacks since the start of February 2022. Recent events, such as the disruption of Satcoms in Ukraine and actions by cyber threat actors, such as the Turla hacking group using satellite-based Internet links [28], along with disruptions to the Global Positioning System (GPS) time signals by other attackers [29], [28], have elevated cybersecurity in the Satcoms domain to a top priority for space-faring nations [30], [21].

Throughout a satellite’s life cycle, both the satellite itself and its Satcoms-related functions depend on secure and reliable cyber capabilities [31], [32]. Given the global nature of satellite and cyberspace operations, international cooperation is imperative to establish a framework of accepted legal rules that safeguard satellites and Satcoms systems from the planning stages to their deployment in space [33], [21], [34]. This emphasizes the need for robust and effective cybersecurity measures to support the progress and continued development of Satcoms in space systems [12], [15].

However, even with the presence of multi-layered security mechanisms in the space industry, Satcoms systems remain vulnerable to escalating cyberattacks [34], [32]. The convergence of the digital realm with the physical dimensions of

TABLE I: Summary of related Satcoms cybersecurity surveys: Coverage of cyberattacks and cybersecurity strategies in the space, ground, and links segments.

Ref.	Pub. year	Survey focus	Cyberattacks			Cybersecurity Strategies			Comments
			Space	Grou.	Links	Space	Grou.	Links	
[35]	2019	Cybersecurity principles for space systems	✓	✓	X	✓	✓	X	Review of causes for the space sector's poor cybersecurity posture, cyberattacks on space systems, and existing mitigation techniques used by space + ground segments.
[36]	2019	Security analysis of a space-based wireless network	X	X	✓	X	X	✓	Summary of security requirements of space-based networks along with three typical attack approaches.
[37]	2020	Satellite-to-satel. cyberattacks, defenses, + resilience	✓	X	X	✓	X	X	Brief description of a new class of satellite-to-satellite cyberattacks along with proposed defense and resilience techniques.
[38]	2020	Security approaches in ML for Satcoms	X	X	✓	X	X	✓	Focus on ML strategies for better security systems in Satcoms.
[39]	2021	Applications of Artificial Intelligence (AI) for Satcoms	X	X	X	X	X	✓	General overview of AI in Satcoms, challenges facing diverse aspects of Satcoms, and their AI-based solutions.
[16]	2021	Cybersecurity in new space	✓	✓	✓	X	X	X	Review of satellite security incidents to assess the motivations and characteristics of adversarial threats to satellites.
[40]	2021	Cybersecurity vulnerabilities for urban air mobility	X	X	✓	X	X	✓	Survey of cybersecurity vulnerabilities and attacks of the commun. systems of aircraft and Unmanned Aerial Vehicles (UAVs).
[41]	2021	Overview of protected Satcoms in intelligent age	X	X	X	X	X	✓	Overview of protected Satcoms systems with a focus on critical technologies and practical applications.
[42]	2022	Cybersecurity challenges in the maritime sector	X	✓	✓	X	✓	✓	Domain (sector)-specific survey of security challenges and mitigation techniques in the maritime sector.
[43]	2022	Cybersecurity in the maritime industry	✓	✓	✓	X	X	X	Classification of cyberattacks within the context of the state-of-the-art in the maritime industry.
[44]	2022	Satellite-based commun. security	X	X	✓	X	X	✓	Survey of links segment security threats, solutions, and challenges.
[45]	2023	LEO satellite security and reliability	✓	X	X	✓	X	X	Survey of LEO satellites with focus on space segment vulnerabilities and approaches for enhancing security and reliability.
Our survey	2023	Architectures of Satcoms segments; corresponding cyberattacks and cybersecurity strategies	✓	✓	✓	✓	✓	✓	Survey of cybersecurity threats and potential cyberattacks associated with each of the three primary segments of Satcoms systems. We comprehensively cover cybersecurity strategies of each architectural segment, along with the key goals for safeguarding Satcoms systems against cyberthreats.

the IoT has brought about covert cyberthreats, demanding novel, efficient, and communicative attack detection mechanisms [46]. Since Satcoms are controlled from the ground and facilitate data transmission to and from the ground, they exhibit various vulnerabilities associated with the IoT that require proactive mitigation [12], [15].

B. Comparison with Existing Surveys

An extensive survey literature covers a wide range of complementary (i.e., non-cybersecurity related) aspects of Satcoms systems, including fifth-generation (5G) and 6G aspects [47], [48], [49], [50], [51] and IoT aspects [52]. Communications for different types of satellites, such as nongeostationary satellites [53] and low-power navigation system satellites [54] have recently been surveyed, as well as the network integration issues arising with satellite networks [55], [56], [57].

Similarly, cybersecurity for general networked systems (not specifically for Satcoms systems) has been extensively surveyed. General cybersecurity threat patterns have been surveyed in [58], [59], [60], while Machine Learning (ML) techniques for networked cybersecurity have been surveyed in [61], [62]. Cybersecurity issues in specialized industrial networks with digital twins have been surveyed in [63], while cybersecurity for Supervisory Control and Data Acquisition (SCADA) systems has been surveyed in [64]. Recently, the security aspects of various forms of 5G wireless networks have been surveyed in [65], [66], [67], [68], [69], [70], [71], while security aspects of 6G networks have been surveyed in [72],

[73], [74], [75], [76], [77].

Table I summarizes the relatively few existing surveys on cyberattacks and cybersecurity in Satcoms systems and contrasts these existing surveys on Satcoms cybersecurity from our survey. In particular, Table I indicates whether each individual survey has covered the cyberattacks and cybersecurity techniques in each individual segment of a Satcoms system. Table I indicates that the existing surveys are generally narrow in scope and do not comprehensively cover the full range of cyberattacks, and cybersecurity techniques for all Satcoms segments within Satcoms systems.

For example, Falco [35] surveyed cyberattacks and cybersecurity techniques up to 2019 for the space and ground segments, while He et al. [36] covered only the links segment. Both Falco [35] and He et al. [36] placed emphasis on the factors that have contributed to the space sector's weak cybersecurity posture. Rath and Mishra [38] as well as Fourati and Alouini [39] focused on ML and Artificial Intelligence (AI)-based strategies for better cybersecurity of the links segment in Satcoms systems, which has also been the focus of Wang et al. [41] and Tedeschi et al. [44]. Manulis et al. [16] gave an overview of past satellite security threats and incidents to understand the motivations and characteristics of adversarial threats to satellites.

The other existing surveys focused on specific application scenarios: Tan et al. [40] reviewed the emergence of Urban Air Mobility (UAM) with the development of high-powered UAVs. Focusing primarily on the links segment, the review [40] covered known cybersecurity vulnerabilities and previous attacks on UAVs and aircraft communication systems, as well as a basic cybersecurity framework for UAM (the related topic of cybersecurity in civil aviation has been surveyed in [78]). Similarly, Akpan et al. [42] and Ben Farah et al. [43] reviewed the current state of the art of maritime cybersecurity and emphasized the importance of addressing vulnerabilities for safe and secure operations in the maritime industry; related IoT aspects have been covered in [79].

While the existing surveys have provided valuable insights into the cybersecurity landscape of various airspace- and satellite-related industries, such as the UAM and maritime sectors, they tend to be limited in their coverage. Specifically, the existing surveys often adopt a selective approach, i.e., do not comprehensively cover the full spectrum of cyberattacks and cybersecurity strategies across all segments of Satcoms systems.

In contrast, our survey takes a holistic perspective by comprehensively covering all three fundamental segments of Satcoms systems: space, ground, and links segments. Each of these segments brings its own set of vulnerabilities and attack vectors, making it imperative to thoroughly comprehend and address the unique challenges they pose. By offering an all-encompassing view of vulnerabilities in each segment, we not only contribute to a comprehensive cybersecurity taxonomy but also provide a deeper understanding of the intricacies inherent in Satcoms systems.

A distinguishing feature of our survey is its in-depth coverage of microservices integrated into Satcoms systems [80]. In the context of Satcoms, microservices refer to small, specialized software modules that play specific roles, such as attack detection [81]. This aspect has been underrepresented in existing surveys. We take a comprehensive approach by highlighting the critical role of microservices and the methodologies they employ, such as Intrusion Detection Systems (IDSs) [82] and Software-Defined Radios (SDRs) [83], in detecting and mitigating attacks across segments and stakeholders.

In contrast to previous surveys, we view microservices as integral components of Satcoms cybersecurity techniques, shedding light on their contributions to the overall security of Satcoms systems. In particular, our survey goes beyond the mere acknowledgment of microservices and presents detailed insights into their applications within various critical areas of Satcoms cybersecurity. This includes their functions in Payload Verification Mechanisms (Sec.V-B1a), onboard Intrusion Detection and Prevention (IDP) (Sec.V-B2), IDP (Sec.V-C3c), and ML applications for Satcoms links cybersecurity (Sec.V-D3). By providing an in-depth survey of how microservices are integrated into these specific domains, we offer practitioners and researchers a valuable resource for enhancing security within each segment of Satcoms systems.

C. Original Survey Contributions and Survey Structure

To effectively address the growing concerns regarding Satcoms cybersecurity and safeguard these critical systems against potential exploitation (abuse) of entry points or vulnerabilities, it is necessary that governments and private sectors collaborate on a global scale [15]. Increased collaboration across these sectors, encompassing hybrid efforts that combine legislative and technical solutions, is a basic strategy for addressing space and Satcoms cybersecurity [16]. In order to inform such efforts, this survey provides a comprehensive account of the state-of-the-art of Satcoms cyberattacks and cybersecurity strategies that should be taken into account by decision-makers, acquisition experts, and system designers when acquiring and designing cyber-resilient Satcoms systems. More specifically, this survey comprehensively presents the cyberattacks on the Satcoms system and the cybersecurity strategies for defending Satcoms systems against cyberattacks in a structured manner, organized by the main architectural segments of a Satcoms system. In particular, this survey is primarily structured according to the architectural segments of Satcoms systems. The cybersecurity aspects of protocols that operate within the Satcoms architectural segments and the resulting Satcoms services are covered within the context of the architecture segments.

We have visually represented the structure of this survey in Figure 3, and we have listed the main abbreviations in Table II. The main original contributions of this survey are:

- Overview of Satcoms architecture: As tutorial background for generalist readers, we provide an overview of the architecture of Satcoms systems consisting of three main segments, namely the space, ground, and links segments in Section III.
- Survey of Satcoms cyberattacks: We comprehensively survey the vulnerabilities and various types of cyberattacks (cyberthreats) that have targeted the three main

architectural segments of Satcoms systems in Section IV. We also classify the different attacker types and explain the consequences of cyberattacks, highlighting the potential consequences for users and organizations, including disruption, economic losses, and loss of life.

- Survey of Satcoms cybersecurity strategies: We comprehensively survey the current state-of-the-art Satcoms cybersecurity strategies, i.e., the general strategies and specific techniques (including the specific microservices) employed to secure the three main architectural segments of Satcoms systems against cyberattacks in Section V. This Satcoms cybersecurity survey includes the use of encryption, authentication, and IDS techniques, as well as the development of secure protocols and standards.
- Learned lessons: In Section VI, we distill the main learned lessons from our comprehensive survey of the Satcoms cyberattacks in Section IV and the cybersecurity strategies in Section V. These main lessons include the need to balance security with cost-effectiveness, the importance of threat intelligence sharing, and the difficulty of securing legacy Satcoms systems.
- Open challenges and future research directions: We highlight the open challenges and future research directions in Satcoms cybersecurity in Section VII, emphasizing the need for continued development of advanced security measures to protect Satcoms against emerging cyberthreats, such as supply chain attacks and software vulnerabilities. We also emphasize the need to improve the resilience of Satcoms against physical attacks.

II. Overview of Satellite Security

Satcoms systems rely on radio waves to transmit information over long distances [84]. Specifically, the satellites in orbit function as relay stations. That is, the satellites receive signals from Earth-based (terrestrial, i.e., on the ground) communication stations, and then actively transfer or pass along these signals to either another terrestrial communication station or to another satellite in space [20]. These signals are often in the form of electromagnetic waves, which propagate through the vacuum of space at the speed of light [85]. The communication systems that rely on satellites have revolutionized many industries, from telecommunications to navigation, and continue to play a vital role in our modern world [6].

Satellite security is a critical issue as satellites are vulnerable to cyberattacks, physical attacks, and space debris [86]. For example, to ensure satellite security, encryption [87], [88] and authentication [89], [90], [91], [92], [93] mechanisms are employed to prevent unauthorized access to the satellite's communication and control systems. Additionally, satellite operators can implement physical security measures to safeguard against physical attacks, such as deploying a protective shield or designing the satellite to withstand high-velocity collisions with space debris [29]. Overall, maintaining satellite security is an ongoing effort, and satellite operators and engineers must remain vigilant to ensure the uninterrupted operation and protection of satellite systems. This section gives a tutorial overview of the space system, Satcoms, as well as the essential security goals for modern Satcoms perspectives.

TABLE II: Summary of main abbreviations

Abbreviations	Meaning
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
C2	Command and Control
CNN	Convolutional Neural Network
DiD	Defense in Depth
DL	Deep Learning
DoS	Denial of Service
DDos	Distributed DoS
FL	Federated Learning
GEO	Geostationary Orbit
GPS	Global Positioning System
GRU	Gated Recurrent Unit
GS	Ground Station
IoT	Internet of Things
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LEO	Low Earth Orbit
MCC	Mission Control Center
NOC	Network Operations Center
OFDM	Orthogonal Frequency Division Multiplexing
OMC	Operations and Maintenance Center
RF	Radio Frequency
Satcoms	Satellite Communications
SCC	Satellite Control Center
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SDR	Software-Defined Radio
TT&C	Telemetry, Tracking, and Command
VLAN	Virtual Local Area Network

A. Space System

Space systems are comprised of space-based assets and land-based infrastructures that collaborate, primarily through Satcoms systems, to accomplish missions in space [15]. Satcoms systems enable critical functions, such as communication, navigation, and weather forecasting, which are relied upon daily. Additionally, space systems advance our understanding of the physical world through celestial observation and planetary exploration [12]. Moreover, space systems' Satcoms provide essential intelligence and monitoring for national security [94]. Due to the high degree of subsystem interactions, minimal design, performance margins, and cybersecurity requirements, space systems often face significant challenges. In particular, cybersecurity has become a critical concern for space systems' Satcoms, especially for those that operate far from Earth [1].

The space industry is a complex system with numerous moving parts, constantly evolving concepts, and shifting dynamics [16]. The space industry encompasses satellite manufacturing, the launch industry, satellite services, and ground equipment, all of which work together to provide space-based services to end-users [20]. During the Cold War era, the space industry was dominated by a few nations and governmental activities, featuring large, costly satellites with long operating lifespans [1]. Information was kept on a need-to-know basis,

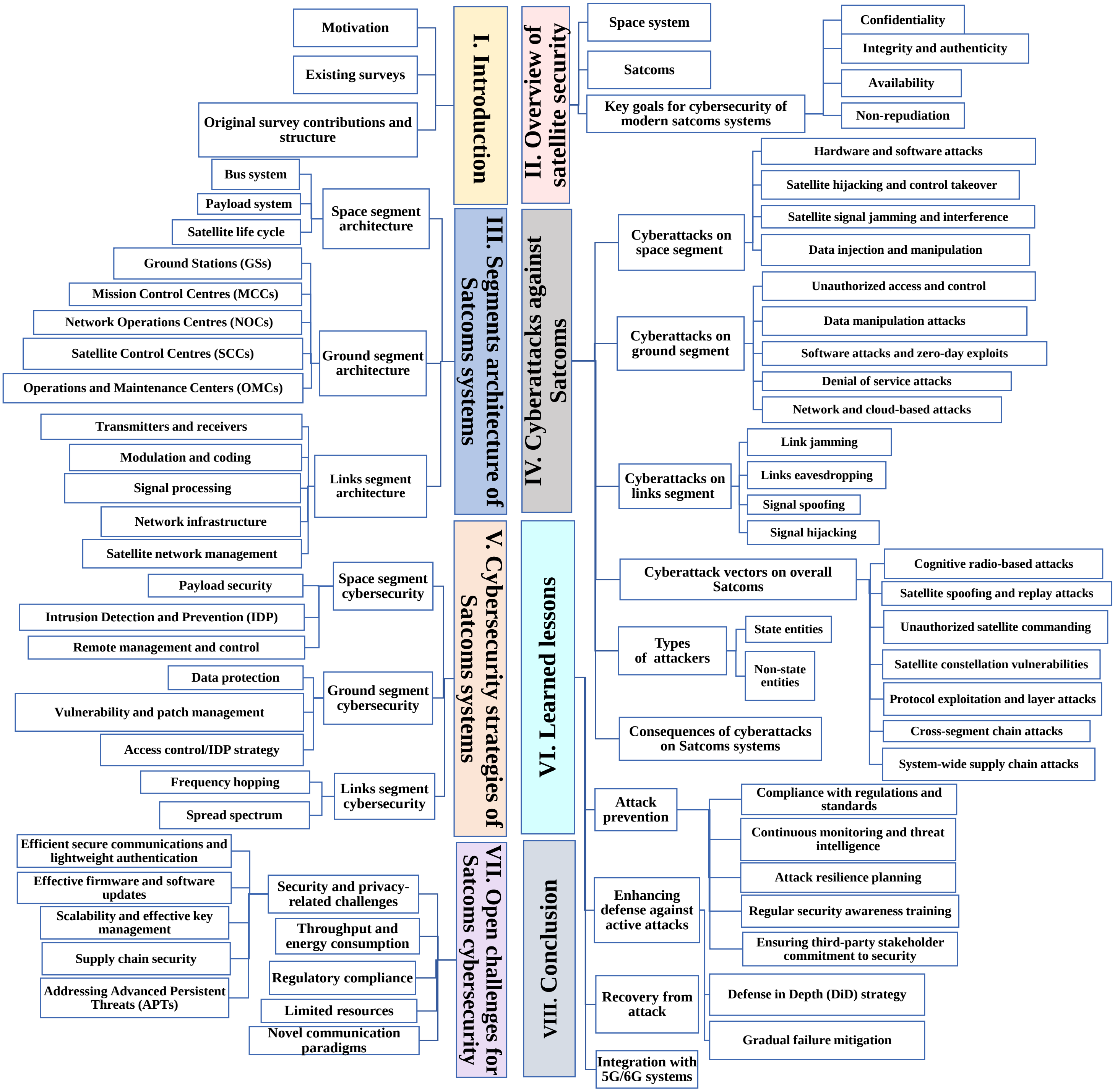

I. Introduction
Motivation
Existing surveys
Original survey contributions and structure
II. Overview of satellite security
Space system
Satcoms
Key goals for cybersecurity of modern satcoms systems
Confidentiality
Integrity and authenticity
Availability
Non-repudiation
III. Segments architecture of Satcoms systems
Space segment architecture
Bus system
Payload system
Satellite life cycle
Ground segment architecture
Ground Stations (GSs)
Mission Control Centres (MCCs)
Network Operations Centres (NOCs)
Satellite Control Centres (SCCs)
Operations and Maintenance Centers (OMCs)
Links segment architecture
Transmitters and receivers
Modulation and coding
Signal processing
Network infrastructure
Satellite network management
IV. Cyberattacks against Satcoms
Cyberattacks on space segment
Hardware and software attacks
Satellite hijacking and control takeover
Satellite signal jamming and interference
Data injection and manipulation
Cyberattacks on ground segment
Unauthorized access and control
Data manipulation attacks
Software attacks and zero-day exploits
Denial of service attacks
Network and cloud-based attacks
Cyberattacks on links segment
Link jamming
Links eavesdropping
Signal spoofing
Signal hijacking
Cyberattack vectors on overall Satcoms
Cognitive radio-based attacks
Satellite spoofing and replay attacks
Unauthorized satellite commanding
Satellite constellation vulnerabilities
Protocol exploitation and layer attacks
Cross-segment chain attacks
System-wide supply chain attacks
Types of attackers
State entities
Non-state entities
Consequences of cyberattacks on Satcoms systems
V. Cybersecurity strategies of Satcoms systems
Space segment cybersecurity
Payload security
Intrusion Detection and Prevention (IDP)
Remote management and control
Ground segment cybersecurity
Data protection
Vulnerability and patch management
Access control/IDP strategy
Links segment cybersecurity
Frequency hopping
Spread spectrum
VI. Learned lessons
Attack prevention
Compliance with regulations and standards
Continuous monitoring and threat intelligence
Attack resilience planning
Regular security awareness training
Ensuring third-party stakeholder commitment to security
Enhancing defense against active attacks
Defense in Depth (DiD) strategy
Gradual failure mitigation
Recovery from attack
Integration with 5G/6G systems
VII. Open challenges for Satcoms cybersecurity
Security and privacy-related challenges
Efficient secure communications and lightweight authentication
Effective firmware and software updates
Scalability and effective key management
Supply chain security
Addressing Advanced Persistent Threats (APTs)
Throughput and energy consumption
Regulatory compliance
Limited resources
Novel communication paradigms
VIII. Conclusion

Fig. 3. Illustration of section structure of this survey.

with the goal of limiting adversaries' knowledge of military capabilities and establishing a framework for secrecy in developmental procedures. The applications that emerged during this period are known as ”Old Space” [22].

Since then, the growth of the consumer electronics sector, advancements in manufacturing processes, and reduced launch costs have transformed space into a highly coveted commercial resource [95], [20]. This private-sector involvement has expanded the scope of the space industry and attracted new companies and initiatives, leading to the coining of the term “New Space” [1], [22]. The concept of New Space embodies the agility pattern that results from combining common units and components to make spaceflight more affordable and accessible across industries [16]. According to [22], this system is also trending towards massive satellite constellations with hundreds or even thousands of satellites and compact satellites (weighing 600 kg or less). Figure 4 illustrates some of the top-level global outcomes that have emerged from the application

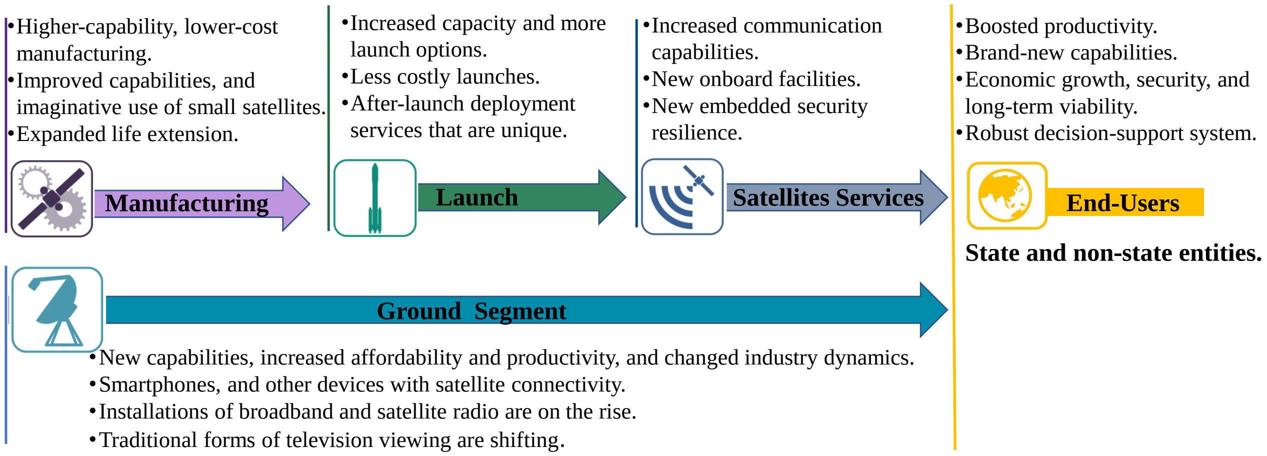

•Higher-capability, lower-cost manufacturing.
•Improved capabilities, and imaginative use of small satellites.
•Expanded life extension.
Manufacturing
•Increased capacity and more launch options.
•Less costly launches.
•After-launch deployment services that are unique.
Launch
•Increased communication capabilities.
•New onboard facilities.
•New embedded security resilience.
Satellites Services
•Boosted productivity.
•Brand-new capabilities.
•Economic growth, security, and long-term viability.
•Robust decision-support system.
End-Users
State and non-state entities.
Ground Segment
•New capabilities, increased affordability and productivity, and changed industry dynamics.
•Smartphones, and other devices with satellite connectivity.
•Installations of broadband and satellite radio are on the rise.
•Traditional forms of television viewing are shifting.

Fig. 4. Global outcomes of new space across several space segments.

TABLE III: Number of active satellites in orbit by major country.

Country	Number of satellites in orbit
U.S.	2944
China	499
Russia	169
Rest of the world	1240

of New Space in several space system segments.

According to a report by Statista [96], there are currently approximately 6,600 satellites orbiting the Earth, with 4,852 of them actively in use. This number continues to grow as more launches take place each year. These satellites serve a variety of purposes, including Earth observation, navigation, technological development and demonstration, space and Earth science, and potentially surveillance programs. Table III illustrates that the United States is the leading country in terms of launching satellites into space, followed by China and Russia, and the rest of the world.

The scientific community is continuously exploring new frontiers in new space by introducing innovative technologies. One such example is the integration of smartphone technology in satellites, which has been successfully demonstrated by missions, such as STRaND-11 [97]. The Earth observation industry has experienced a boom in investments due to the extensions of satellite imaging and signals intelligence, leading to the development of corporate intelligence products [27] and environmental conservation activities. Moreover, the new space era is witnessing the emergence of worldwide broadband Satcoms services [16]. These services aim to provide access to remote and rural areas while offering fault-tolerant networks for critical services. Over the past five years, Satcoms broadband income has been steadily increasing and is projected to grow even faster with the launch of satellite constellations, such as Starlink, OneWeb, and Telesat, which are expected to feature hundreds or even thousands of satellites [2], [96], [27]. Moreover, various industries have consistently integrated satellite geolocation capabilities to enable route mapping, fleet monitoring, and time-sensitive objectives in the commercial and power sectors.

In recent years, Satcoms have played an increasingly crucial role in modern warfare. The origins of military space and Satcoms date back to the Sputnik crisis in October 1957 [94], which triggered the space race between the Soviet Union and the United States. More recently, many governments have pursued military applications of space. For instance, in March 2019, India conducted an anti-satellite weapon test, while Iran launched its first military satellite in April 2019 [98]. In 2015, China established the strategic support force, which covers space, Satcoms, and cyber operations, and Russia established an autonomous space force. In response to these developments, France formed a space command in September 2019, while the United States established a space force in December 2021 [99]. These military systems have to meet stringent cybersecurity standards and utilize encryption, anti-jamming measures, and robust Satcoms, among other technologies [16].

B. Satcoms

Satcoms, formally known as Satellite Communications, refers to the transmission of data, voice, video, and other communication services via artificial satellites that orbit the Earth [96], [17], [100]. Satcoms technology involves the use of ground-based (terrestrial) stations to send and receive signals to and from satellites. The satellites act as relay stations in space, facilitating communication over vast distances. Satcoms systems play a crucial role in various applications, including telecommunications, broadcasting, remote sensing, navigation, and scientific research [12], [6], [11].

According to the Radio Regulations (RR) of the International Telecommunication Union (ITU), Satcoms systems are classified into two categories, fixed satellite service and mobile satellite service [11]. Fixed satellite service refers to the provision of communication services between stationary stations, while mobile satellite service involves the provision of communication services between moving stations, such as aircraft, ships, and automobiles. Another mode of communication that involves the direct reception of radio transmissions from space stations to the ground is known as satellite broadcasting, which is classified as broadcasting satellite service as per the RR [41].

In recent years, Satcoms systems have become an integral component of aerospace communications, especially in oceanic airspace. The increasing demand for airborne connectivity and the rapid development of new technologies are expected to make Satcoms as important in the continental airspace in the future as they are currently in the oceanic airspace. In fact, Satcoms are projected to become a critical element of the Future Communications Infrastructure (FCI) [6], which is designed to meet the current and future communication needs of the aerospace industry. With the increasing deployment of satellite constellations, new Satcoms systems with advanced capabilities are being developed to cater to the diverse communication requirements of the aerospace industry.

In space exploration, Satcoms systems are crucial. Watching Apollo 11 landing on the Moon, getting Pluto's images from a new horizon, having scientific data from Rosetta, and directing Voyager 1 to tilt its camera and capture a record-breaking photo of Earth from a distance of roughly 6 billion kilometers, all of these accomplishments, as well as a slew of others, would not have been feasible without extremely effective Satcoms between Ground Stations (GSs) and the space explorers [6]. The space exploration era began in 1957 with the launch of Sputnik [94], and has continued to this day mostly through robotics missions or short human flights beyond Earth's orbit, such as the Apollo program [101].

The current paradigm shift in space operations is commonly summed up by the term "Space 4.0" [102], in which many space organizations aspire to establish a sustained human presence on other celestial planets in the space system. The "Moon Village" vision proposed by ESA [103] is promising in this regard since it aims to translate this paradigm shift into a series of actual activities and establish an environment where both global collaboration and space commerce may bloom.

Such a grand vision can only be realized if high-capacity, highly reliable, and secure Satcoms links are constructed between the Earth and the communicating elements around the space system [6], [102], [103]. Due to the vast distance between the Earth and the satellites, effective cybersecurity systems are needed to address both the cyberthreats and the security concerns that arise in typical Satcoms systems. This, along with the restricted power that a satellite can produce far from the sun, introduces new communications cybersecurity requirements that are substantially different from those on Earth. Moreover, as Satcoms evolve and billions of devices connect to ever-expanding networks, security, and privacy are emerging as major concerns.

C. Key Goals for Cybersecurity of Modern Satcoms Systems

This section presents the fundamental security objectives essential for bolstering the cybersecurity of modern Satcoms systems, including those aligned with the New Space concept. The contemporary landscape of Satcoms systems is witnessing increased congestion, contention, and competitiveness, given their pervasive utilization in both civilian and military realms [94], [99], [43]. As the new space domain evolves beyond the exploration phase, there arises a critical need to establish a robust cybersecurity framework for Satcoms systems [104], [28]. To meet this objective, it is imperative to delineate and prioritize common key goals, as visually depicted in Figure 5. These key goals collectively form the foundation for ensuring the reliability and comprehensive protection of Satcoms systems [105].

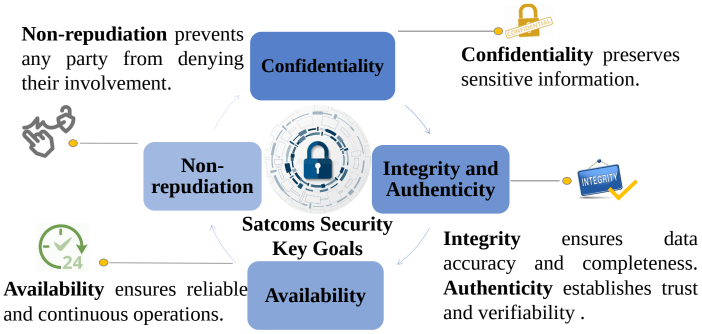

Non-repudiation prevents any party from denying their involvement.
Confidentiality
Confidentiality preserves sensitive information.
CONFIDENTIAL
Non-repudiation
Integrity and Authenticity
INTEGRITY
Satcoms Security Key Goals
24
Integrity ensures data accuracy and completeness. Authenticity establishes trust and verifiability .
Availability ensures reliable and continuous operations.
Availability

Fig. 5. Key cybersecurity goals of modern Satcoms systems.

1) Confidentiality: Confidentiality involves safeguarding sensitive information and upholding authorization constraints on its access and disclosure [106], [105], [66]. While confidentiality has historically not been a significant concern in Satcoms systems, the proliferation of readily available technology has made it easier for unauthorized parties to eavesdrop on active Satcoms channels and to intercept unencrypted space-ground data communications [44]. Voice-based communication, which is still widely used in Satcoms systems, particularly in situations where direct communication is required between individuals or groups, has not been designed with confidentiality as a priority. Therefore, the confidentiality of Satcoms links can be easily compromised if adequate measures are not taken to secure these communications [107].

While much of the data transmitted between satellites and the ground may not be confidential in the sense of personal or classified information, this does not imply that sensitive information is never sent over Satcoms network channels [105]. Also, the satellites and onboard equipment store significant quantities of operational data that, provided appropriate confidentiality is guaranteed, may be made available to pertinent individuals on the ground. Ensuring that such information is kept confidential will stop it from being disclosed to unauthorized parties who may be illegally listening in on the Satcoms channels. A Satcoms system without assured confidentiality allows attackers to map any potential vulnerabilities [104], [105], thus compromising the cybersecurity of the overall Satcoms system.

2) Integrity and Authenticity: Ensuring data integrity in modern Satcoms involves guaranteeing the completeness and accuracy of transmitted information [106]. In the realm of cybersecurity, this means preventing any unauthorized party from covertly intercepting and altering messages exchanged between, for instance, a satellite and the controlling GSs. Properly established data integrity protocols are essential to thwart undetected manipulation of data [105].

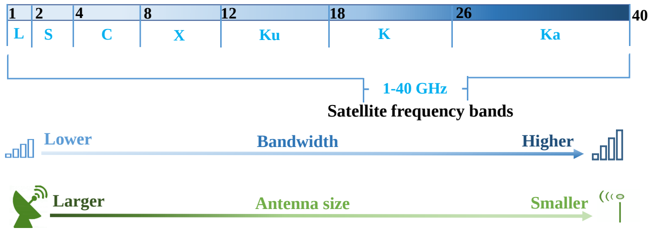


Fig. 6. Frequency bands for Satcoms.

Authenticity, on the other hand, refers to the quality of being genuine and verifiable. Trust in the legitimacy of a transmission, message, or its source is closely tied to integrity. This process entails authenticating the origin of the information or verifying the claimed identity, and it goes beyond mere detection algorithms, such as hash encryption algorithms [41] and Cyclic Redundancy Check (CRC) [108].

In Satcoms systems, ensuring the integrity and authenticity of data transmissions to control GSs is crucial and will continue to be so [36]. While the conversational context in a speech signal provides some assurance for integrity and authenticity, data transmissions lack inherent indicators in a correctly structured and contextually appropriate message to confirm the legitimacy of the transmitter or to reveal potential alterations during transmission [36]. To elaborate, maliciously modified data messages may appear legitimate, posing a serious concern as modern Satcoms systems increasingly rely on data transmissions rather than voice commands (which were often used in the past to control satellites) [105]. In this scenario, messages from unfamiliar sources could potentially deceive the receiving satellite into executing risky commands [24]. However, the shift to data transmissions in contemporary Satcoms systems is motivated by the enhanced security and reliability of contemporary Satcoms systems, allowing for more precise control over satellite operations. Nevertheless, the inability to verify the authenticity of a data message carrying command and control instructions can lead to severe consequences [49], [24].

3) Availability: From the standpoint of cybersecurity, availability is ensuring that all systems are operational and functional whenever necessary, regardless of the situation [106]. Availability is a key consideration for the majority of services that use the Satcoms links. For instance, keeping the service from being interrupted and ensuring that pertinent information from the spacecraft can reach the ground segment (service providers) will preserve end-user safety. Today, many airlines rely on Satcoms links, and the breakdown of such a link means that airlines' flight schedules may be delayed [110].

In the domain of Satcoms, availability is a well-established concept often factored into the formulation of safety and performance standards [36]. However, safety hazard assessments within this context tend to primarily focus on accidental message losses and arbitrary system component failures. Consequently, design decisions derived from safety hazard assessments typically lack explicit considerations of defenses against deliberate malicious attacks. These malicious attacks may include, but are not limited to, Denial of Service (DoS) attacks and purposeful jamming of Satcoms links [111], as comprehensively surveyed in Section IV. It is important to note that this observation about the primary focus on message losses and component failures holds true for many New Space Satcoms systems, such as CubeSats [112], [113]. In contrast, broader safety designs in domains, such as maritime and aviation, inherently integrate security considerations against intentional adversarial actions in the evolving landscape of Satcoms cybersecurity [40], [43], [42].

4) Non-repudiation: Non-repudiation protects all parties participating in a communication exchange from the event that one of the parties denies taking part in all or a portion of the communication exchange [110]. Non-repudiation precludes either the sender or the receiver from disputing the origin and/or delivery of a message [105]. Ensuring non-repudiation also entails being able to demonstrate with legal authority whether an incident occurred or not, as well as whether a party was involved or not. Although authenticity and non-repudiation are closely related notions, techniques that offer authenticity may not always provide non-repudiation and vice versa [36].

Non-repudiation is currently a little-known term in Satcoms systems, since non-repudiation is not directly related to safety. According to the FCI [106], it should be possible to uniquely trace an entity's actions so that the entity can be held accountable for its activities, and responsibility for actions undertaken is introduced as a specialized criterion. From a security standpoint, there are likely to be many instances where the parties participating in a Satcoms system or application data transmission would like to prove—in retrospect—that a specific actor transmitted a particular message. It may be crucial to be able to identify the responsible party if, for instance, a signal about satellite operations delivered from the ground to a spacecraft causes serious damage, communication delays, or other financial effects [36]. Non-repudiation may therefore be significant from a legal perspective, even though it may not be relevant from an operational safety perspective [110].

III. Segments Architecture of Satcoms Systems

This section describes the Satcoms system architecture and segments. We also provide an overview of the main satellite life cycle phases.

A. *Overview of Satcoms Systems Architectures*

A common configuration for Satcoms systems consists of a space segment and a ground segment that communicate with each other using Radio Frequency (RF) transmissions [35]. The space segment is one of the three critical operational components of Satcoms systems. The space segment includes satellites or groups (constellations) of satellites in orbit [6] and launchers designed to deploy satellites into space. A satellite constellation is an artificial satellite group that functions as a single unit [16]. Constellations, unlike single satellites, provide nearly continuous global coverage, ensuring that at least one satellite is visible anywhere on Earth at any given time [44].

TABLE IV: Radio frequencies for Satcoms and applications.

Satellite freq. [GHz]	Band	Applications
1–2	L	Carriers for the Global Positioning System (GPS), satellite mobile phones, such as Iridium and Inmarsat, which offer communication services for sea, land, and air, and World Space satellite radio.
2–4	S	Weather and surface ship radar, as well as some communications satellites, e.g., NASA satellites for communicating with the International Space Station (ISS).
4–8	C	Satellite television networks operating on a full-time basis, or unprocessed satellite feeds.
8–12	X	The applications of radar technology include military purposes, weather monitoring, as well as traffic control for airplanes and ships. Various types of radar are used, such as continuous-wave radar, pulsed radar, single-polarization radar, dual-polarization radar, synthetic aperture radar, and phased arrays.
12–18	Ku	Services provided by communication and broadcast satellites, such as Astra.
26–40	Ka	Satcoms, radar altimeters, certain types of weather radar, and satellite-based surveillance systems [109].

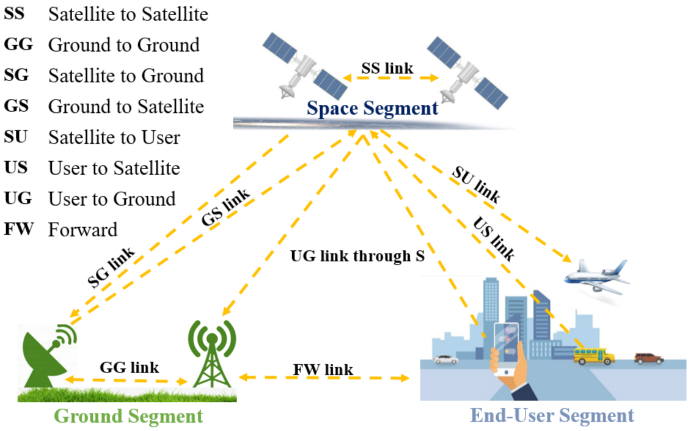


Fig. 7. Satcoms architecture with three main segments: the space segment, ground segment (which includes the end-user segment), and the links segment.

Satellites are typically positioned in groups of complementary orbital planes to connect with widely dispersed GSs [114]. Generally, a satellite is mainly composed of a payload, which is the equipment that executes the satellite's mission, and a bus, which houses the payload and other satellite systems [16].

Satcoms systems employ RF waves, typically in the Megahertz (MHz) and Gigahertz (GHz) frequency range, to communicate with satellites. The uplink channel is used to transmit signals from Earth to the satellite, while the downlink channel is used to transmit signals from the satellite to Earth. To minimize interference both on the ground and in space, Satcoms uplink and downlink channels commonly use different frequencies [17]. The Federal Communications Commission (FCC) and the ITU have authorized the bands, frequency regulations, and recommendations for communications in general, including Satcoms [11]. For instance, the Satcoms frequency bands are standardized to be within the range of 1 to 40 GHz, as specified by the ESA [44], see Table IV and Figure 6.

A Satcoms system's reference communication architecture, as shown in Figure 7 typically consists of: (i) A space segment that includes the satellites and the Satellite to Satellite (SS) links. (ii) A ground segment, which is operated by the operators of the satellites (or network gateways) and allows for the Ground to Ground (GG) and Forwarding (FW) links which are actual terrestrial links that transmit data originating from the satellites to the end-users on the ground. The ground segment also includes the end-user segment, which consists of the end-user terminals, such as smartphones, ships, and airplanes. (iii) A links segment, which encompasses all the links between the space segment and the ground segment; this involves Satellite to Ground (SG), Ground to Satellite (GS), Satellite to User (SU), User to Satellite (US)links, as well as User to Ground (UG) links through satellites links [44].

One of the three key elements of Satcoms architecture is the space segment. GEO satellites for navigation, data, and radio broadcasting systems are included in this segment. MEO satellites are also being put into operation at the same time to support network connectivity in the avionics and maritime domains and to provide service providers, government organizations, and businesses with low-latency, high-bandwidth data connectivity. LEO satellite constellations are used for a variety of other applications as well, including imaging, broadband internet, and low-bandwidth telecommunications. A launch vehicle places each of these satellites into orbit. Military and defense Satcoms systems, as well as commercial Satcoms transponders and payloads, are all part of this space segment [6].

The establishment of communication between the satellites and the terminals in the user segment is facilitated by the ground segment. For this, the ground segment includes dedicated gateway stations (such as satellite GSs), control infrastructures, and network operation centers [such as the Network Control Center (NCC) as well as the Network Management Center (NMC)] that assist with user requests for satellite access [100].

The end-user segment in the ground segment includes the user terminals, e.g., ships, airplanes, and satellite phones. While their communication with the gateways can occur over any communication technology, these devices can communicate with satellites by taking advantage of the link between the ground segment and the end-user, such as the Forward (FW) link. The forward link is made up of two parts: an uplink (US,

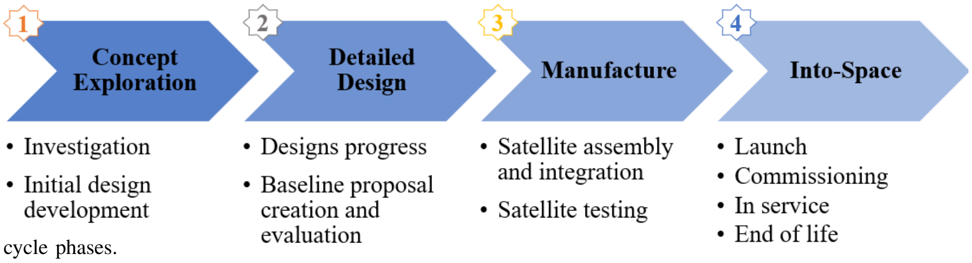


Fig. 8. Satellite's life cycle phases.

from the end-user terminal to the satellite) and a downlink (SU, from the satellite to the end-user). As an alternative, some constellations, such as LEO constellations (e.g., Iridium, Globalstar, Thuraya, and Inmarsat), permit direct user-handset connections to the satellites using the US link [44].

B. Architectures of Space Segment

A space segment is made up of different systems. Each system serves a distinct purpose and may be divided into two main categories: satellite bus systems and payload systems [115]. The bus system components of the satellite perform all the necessary activities for the satellite to remain in orbit and maintain the payload [116], [117]. Power generation and distribution, thermal control, communications systems, attitude and orbit control, the onboard computer, and other systems are part of the bus system [118] and are further detailed in Table V.

The payload system of a satellite plays a crucial role in its mission, as it is responsible for the specific tasks and functions the satellite is designed to perform [122]. Depending on the mission type, the payload can vary significantly. For example, in a scientific satellite, the payload may consist of advanced instruments, such as telescopes, sensors, and processors [120]. These instruments are designed to capture scientific data from space, such as images of celestial objects or measurements of various physical phenomena [6].

In the context of Satcoms, the payload can be classified into two main categories: transparent and regenerative [6].

- Transparent Payload [122]: The primary function of a transparent payload is to relay signals. The transparent payload does not actively process the signals it receives. Instead, the payload amplifies and retransmits the signals to the ground without significant modification. Transparent payloads are often used in simple communication scenarios where the satellite's role is to extend the range of communication links [6]. For instance, a transparent payload may be employed for basic data relay or broadcasting purposes. These transparent payloads typically do not require dedicated onboard processors.
- Regenerative Payload [6]: In contrast, a satellite with a regenerative payload has more advanced processing capabilities on board. When it receives signals from the ground or other satellites, the regenerative payload actively processes these signals. This can involve demodulation, error correction, data optimization, and even frequency band conversion [122]. Regenerative payloads are used in complex communication networks and scenarios where signal quality, data integrity, and flexibility are critical. These regenerative payloads often have their own dedicated onboard processors to handle the extensive data processing tasks before retransmitting the signals [6].

Typically, a satellite's life cycle is divided into four distinct phases, as illustrated in Figure 8. The system will go through a number of technical tests at the end of each phase before moving on to the next phase to confirm that the phase has been adequately accomplished and that the system is ready to go on [16]. The concept exploration is the initial phase. During this phase, the viability of the primary mission concept will be investigated, and an initial design will be created. The customer's requirements must be considered in this initial design. The detailed design is the second phase. As the mission and satellite designs progress, the customer may offer more specific requirements. A baseline proposal for the mission will be created by the end of this detailed design phase. This baseline proposal serves as a jumping-off point for the following manufacturing phase. However, before moving on to the next phase, the design must pass another round of evaluation.

The overall satellite design is finished and the manufacturing commences in the third step, which is the manufacture and test phase. A satellite's many components are frequently provided by a variety of different suppliers [19]. The satellite manufacturer's goal is to assemble all individual pieces in the satellite assembly and integration phase [16]. Satellites must be manufactured in clean rooms, which are sterile settings.

To guarantee that the satellite can withstand both the launch and the hostile environment of space, it must go through a series of tests [16]. The satellite will be brought to the launch site and incorporated into the launcher once it has completed all tests. Final tests will be performed to ensure that all satellite systems are in good working order, as well as to fill and test the satellite's own fuel tanks for any leaks. After that, the satellite and launcher will be ready to go. Finally, the satellite will be sent into orbit from its launchpad [94].

The mission-specific duration of a satellite's functioning is significant, although the satellite's life cycle after manufacturing follows a common pattern of launch, commissioning, in-service, and end-of-life [16]. All of those sub-stages form the fourth phase, which is the into-space phase. More specifically, after loading the satellites onto a launcher and sending them into orbit, the launcher will release the satellites after attaining the intended point, which may have been shared by numerous operators. Then, the commissioning starts, which is the process

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2024.3408277

TABLE V: Satellites' subsystems categories.

System Category	Subsystems	Subsystem's Responsibilities
Bus systems	Power system	Earth-orbiting satellites generate power with large solar panels. Rechargeable batteries allow for power to be stored and used as needed, including during periods of the eclipse when the Earth blocks the satellite's view of the Sun [119].
	Thermal Control System	This system regulates the temperature of satellite systems to ensure their proper operation [118] at the temperatures in space [120].
	Attitude and Orbit Control System (AOCS)	The AOCS controls the satellite's orbit and its attitude (orientation) [121] so as to direct the satellite antennas towards the Earth for communication with GSs, and the solar panels towards the Sun for power generation. Star sensors provide information on the satellite's position, while actuators, such as small thrusters and wheels, generate torque to rotate the satellite as required [6].
	Satcoms systems	Satcoms technology facilitates bidirectional commun. between the satellite and Earth's GSs [6]. Ground commands, known as telecommands, are sent to the satellite, which responds with telemetry data and information relayed to the GSs. The spacecraft's external commun. antennae utilize RF to transmit this data [120].
	Onboard Processor	The onboard processor serves as the "brain" of the satellite [84], responsible for managing both the data received from GSs and from the satellite's own systems. Upon receiving commands from the ground, the onboard processor categorizes the information into specific groups before directing them to the appropriate systems. Additionally, the processor collects data from multiple systems, organizing the data into packets that are transmitted to GSs via the Satcoms system [15].
Payload system	Dedicated onboard processors	In addition to the satellite bus's processor, dedicated onboard processors are often installed for payloads. These processors are utilized to handle the vast quantities of data collected by the payloads before transmitting the data to the ground [120].

of placing the satellite in its proper orbit so that normal activities may begin. In the commissioning phase, the satellite will navigate itself into the proper orbit and prepare for its normal mission.

Over a few months, the ground segment begins to observe and manage the satellite via Telemetry, Tracking, and Command (TT&C) Satcoms systems, and the correct functioning of satellite subsystems is checked in preparation for in-orbit operations [94]. After that, the satellite enters operation and performs its assigned mission until it is decommissioned. During its core lifetime, the satellite will be employed in normal operations, with GSs managing TT&C to keep the satellite running and the payload operational [6]. Finally, the satellite is shut down by commands issued from the ground at the termination of its mission. Eventually, the satellite is instructed (via the Satcoms links) to reach either a higher orbit or a lower orbit (where it will burn up in the atmosphere) [16].

C. Architectures of Ground Segment

Depending on the required communication interfaces and envisioned Satcoms system services, the ground segment architectures vary greatly [121]. The ground segment includes all ground-based elements of a space system used by providers and support systems. The ground segment enables the management of the spacecraft. Also, the ground segment distributes the payload and telemetry data to terrestrial users [123]. A ground segment's primary components are:

- GSs connect via radio transmissions to the spacecraft so as to conduct TT&C, as well as to transmit and receive payload data [94]. Typically, a primary GS and multiple backup GSs maintain radio contact with a satellite to ensure reliability in case of terrestrial natural disasters [69].
- Mission Control Centers (MCCs, typically multiple for reliability) [123] collect and analyze the telemetry data from the satellite. Based on the telemetry data, the MCCs issue commands to control and configure the satellite. Also, the MCCs update the satellite software and archive relevant operational data.
- Network Operations Centers (NOCs) [124] are the central hubs of the ground segment and perform the overall network management and control. NOCs oversee the operations of the GSs, monitor the system's performance, and provide support to end-users.
- Satellite Control Centers (SCCs) [124] are specialized centers that manage and control the operations of the satellite, including its orbit, attitude, and payload. SCCs communicate with the satellite and send commands to it to perform specific tasks.
- Operations and Maintenance Centers (OMCs) [124] are responsible for the maintenance and upkeep of the ground segment components, including the GSs, network infrastructure, and other support equipment.
- User Terminals which are the devices used by the end-users to access the Satcoms network [125]. User terminals include handheld devices, mobile phones, laptops, and other devices.

Network operations and TT&C can be separated from the communications that relate to the service provided by Satcoms systems [124]. Users can access data either directly from a satellite to a specific receiver device or indirectly through a gateway GS that transmits data from its connection with a satellite to an interface over terrestrial networks [16].

D. Architectures of Links Segment

The links segment in Satcoms systems refers to the communication links between the ground segment and the space segment, including the links between the GSs and the satellites. The architecture of the links segment typically includes the following components:

- Transmitters and receivers: These components transmit and receive signals between the ground segment and the space segment. The transmitters and receivers may include RF equipment, antennas, modems, and other components [84].
- Modulation and coding: The modulation and coding techniques used in the links segment are critical for ensuring the reliability and security of the communication links [84]. These techniques encode the data being transmitted and modulate the carrier signal used to transmit the data.
- Signal processing: The signal processing component of the links segment processes the data received from the satellites, removes any noise or interference in the signal, and decodes the data for further processing [122].
- Network infrastructure: The links segment is supported by a network infrastructure that includes routers, switches, and other equipment used to manage the communication links between the ground segment and the space segment [84].
- Satellite network management and operation: The management and operation of the satellite network is critical to ensure the efficient and reliable operation of the communication links [121]. This includes network protocols for the scheduling of the communication links, the monitoring of the network performance, and the management of the network resources [6]. Due to the significant propagation delays of satellite links, conventional network protocols may need to be adapted for the operation in Satcoms [126], [127], [128], [129], [130], [131].

All segments, along with the entities they contain, represent vulnerabilities in Satcoms systems [15]. Since attacks can be launched in any of these outlined segments, cybersecurity is a concern. Therefore, regardless of the target location, the ground segment should be appropriately secured and any communications coming from the satellite should be protected.

E. Summary and Discussion

This section provided an overview of the components of Satcoms systems, which are crucial for satellite-based communication systems to function properly. Satcoms systems are typically composed of two primary segments, namely the space segment and the ground segment, which communicate with each other via RF transmissions in the links segment.

As explained in Section III-B, the space segment comprises satellites or groups (constellations) of satellites in orbit, providing uninterrupted global coverage to ensure that at least one satellite is visible from any point on the Earth's surface at any given time. On the other hand, the ground segment, as seen in Section III-C, encompasses all ground-based components used by providers and support systems, such as GSs, MCCs, NOCs, SCCs, OMCs, and user terminals. These components are crucial for spacecraft management and the distribution of payload data and telemetry to interested parties on the ground.

The links segment refers to the communication links between the ground segment and the space segment, which include the links between the GSs and the satellites. The links segment's components, including transmitters and receivers, modulation and coding techniques, and signal processing, ensure the reliability and security of the communication links have been covered in Section III-D.

Understanding the architecture and segments of Satcoms systems is essential for designing, developing, operating, and securing satellite-based communication systems [34]. The common configuration of Satcoms systems ensures seamless communication between the space segment and the ground segment, allowing for continuous, reliable, and secure communication [114].

IV. Cyberattacks Against Satcoms Systems

Since their inception, Satcoms systems have been subjected to a number of attacks by a variety of adversaries for a variety of reasons [44], [29]. In late February 2022 [138], a cyberattack impacted the international satellite Internet and TV provider Viasat. The attack disrupted services on February 24, coinciding with Russian forces' assaults on Ukrainian cities. Although as of this writing, the full extent of the attack has not been quantified, initial evidence suggests that Internet service has been cut off for thousands of customers in Europe. As per joint French, Ukraine, and United States intelligence, the attack successfully disabled modems to the extent that they could not be turned on, and would need to be reprogrammed, or in some cases, replaced [18]. The current belief is that malware had allowed the attackers, who had likely already gained access to Viasat networks, to purposefully manipulate the modems. Despite the conflict in Ukraine and the impact that resulted, the joint intelligence effort has not attributed the attack to Russian state entities.

On March 17, 2022, the U.S. Department of Homeland Security (DHS) issued an alert advocating the strengthening of Satcoms network provider cybersecurity, no doubt in response to revelations of the Viasat incident [139]. The cyberthreat to satellites has been a longstanding concern and one that has, unfortunately, got mixed in with the myriad of other cybersecurity issues facing the global community [12]. As a result, it is not surprising that satellite security has been neglected, particularly given the need to prioritize and safeguard a total of 16 critical infrastructure sectors [15].

According to the CyberPeace Institute [18], there has recently been a significant escalation in the number of reported cyberattacks against Satcoms providers [86]. Ukraine's Satcoms systems, for instance, are no strangers to being the target of such cyberattacks; as illustrated in the timeline in Figure 2.

This section surveys the vulnerabilities of the Satcoms segments, as well as the different types of attacks that Satcoms systems have experienced and the motivations behind the attacks. Thus, this section reviews the security threats and the likelihood that they could be used against Satcoms systems.

TABLE VI: Definitions of the threat classifications in the STRIDE model [132], [133], [110], [134], [135], [136].

Threat Classification	Definition
Spoofing	Cyberattackers masquerade as legitimate entities or sources to deceive systems and users, gaining unauthorized access or manipulating data [44].
Tampering	Unauthorized modifications or alterations to data, software, or hardware components with malicious intent to disrupt or compromise system integrity [110].
Repudiation	Denial or rejection of responsibility for actions, i.e., attackers try to evade accountability, leading to potential disputes and challenges in attributing actions to specific individuals [110].
Information Disclosure	Unauthorized access or exposure of sensitive information, leading to potential privacy breaches, data leaks, or the misuse of confidential data [105].
DoS	Cyberattackers overload systems or networks with malicious traffic or requests, causing legitimate users to be denied access or experiencing significant performance degradation [137].
Elevation of Privilege	Attackers exploit vulnerabilities to gain higher privileges or access rights than they are authorized to have, enabling them to perform unauthorized actions and to control a system or network [110].

A. Organization of Survey of Satcoms Cyberattacks

1) Overview of Satcoms Vulnerabilities: Satcoms systems operate both in space and on the ground, creating multiple potential points of entry that could be targeted by cyberattackers, as shown in Figure 1. Consequently, accessing the Satcoms networks is often easier than it would be if there was only one point of entry to defend [15]. For a potential cyberattack, there are three key points of entry:

1) Space segment (Section III-B): includes the individual satellites (spacecraft) in orbit that provide the communication links between the ground segment and end-users. Satellites are vulnerable to cyberattacks, as they may rely on software, firmware, and communication protocols that could be exploited by attackers to gain unauthorized access or to manipulate the satellite's operations [36], [140], [141].
2) Ground segment (Section III-C): includes all the land-based infrastructure components, such as GSs, that support space-based assets [16]. As the ground segment manages the communication links with the satellites, the ground segment components are convenient entry points for attackers that seek to disrupt the controlling and monitoring of the satellite's operations, as well as the processing and distribution of the data received from the satellite [16].
3) Links segment (Section III-D): refers to the communication links between the ground segment and the satellite, the satellite-to-satellite links, as well as the links between the satellite and the end-users. These links may be vulnerable to interception, eavesdropping [67], [142], manipulation, and disruption, which could result in the loss or manipulation of data, unauthorized access to the system, or the loss of control of the satellite [6].

Each of these points of entry represents a potential target for attackers, making it essential to implement comprehensive security measures to mitigate the risks of cyberattacks [15]. Additionally, the supply chain factor is critical as satellites involve numerous manufacturers and a structure integrator to function as a cohesive unit [35]. The involvement of diverse vendors provides multiple avenues for attackers to gain access. While military satellites prioritize cybersecurity and employ advanced cryptographic techniques and secure GSs [94], civilian satellites may be more vulnerable to hacking [16].

Previously, space-based assets were primarily targeted by state entities, but the accessibility of computer hacking technologies has lowered the technological barrier, enabling a broader range of potential attackers. As a result, state-of-the-art supervision and safeguarding procedures are now essential for Satcoms-based systems, similar to other systems that handle vital assets [44].

Understanding the distinct vulnerabilities of the Satcoms space segment, ground segment, and links segment is crucial for comprehensively addressing potential cyberthreats [110]. We will present real-world examples and provide insights into how these attacks may impact Satcoms infrastructures and services. Additionally, we will highlight the significance of secure supply chain practices and the growing importance of robust cybersecurity strategies in the face of evolving threats.

2) Taxonomy Scheme of Satcoms Cyberattacks: We organize the survey of the potential cyberthreats (attacks) that target Satcoms systems according to the Satcoms segment, as summarized in Table VII. Specifically, Section IV-B surveys cyberattacks targeting the space segment, while Section IV-C covers the ground segment, and Section IV-D covers the links segment.

Within a given Satcoms segment, we organize the Satcoms cyberattacks according to the categories of the existing Satcoms-specific cyberattacks; whereby, we distilled the categories of Satcoms-specific cyberattacks from a comprehensive review of the existing literature by striving to create a logical categorization that comprehensively covers all existing attacks. We order (sequence) the categories of Satcoms-specific cyberattacks for a given Satcoms segment according to the general theme of progressing from hardware to software and then to signal/data in terms of the considered entity, in combination with a general ordering theme that progresses from an individual component to the broader overall system or the involvement of a network of satellites or communicating nodes.

Within each category of Satcoms-specific cyberattacks, we indicate the corresponding classifications within the STRIDE model, which is a widely recognized general framework for categorizing and analyzing security threats [132], [133],

TABLE VII: Summary of organization scheme of cyberattacks on Satcoms systems according to categories of Satcoms-specific cyberattacks, with mappings to corresponding cyberthreats in STRIDE model [132], [133], [110], [134], [135], [136].

Satcoms-Specific Attack Category	**Corresp. STRIDE Model Classification**	**Attack Description**	**Key Attack Characteristics**
Cyberattacks on Space Segment, Sec. IV-B			
Hardware and Software Attacks, Sec. IV-B1	Tampering, Information Disclosure, Elevation of Privilege	Attacks targeting satellite hardware and software.	Use of malware, DoS attacks, and exploitation of COTS components, hardware, or software failures.
Satel. Hijack., Control Takeover, Sec. IV-B2	Spoofing, Elevation of Privilege	Unauthorized control over satellites.	Exploiting commun. protocol and command interface vulnerab., spoofing techn.
Satel. Signal Jamming and Interf., Sec IV-B3	DoS, Tampering	Deliberate disruption of satellite signals.	Flood communication channels with interference signals.
Data Inject, and Manip., Sec. IV-B4	Tampering, Information Disclosure	Injecting malicious data and manipulating transmissions.	Misleading ground control, altering data, unauthorized access to sensitive info.
Cyberattacks on Ground Segment, Sec. IV-C			
Unauthorized Access and Control, Sec. IV-C1	Elevation of Privilege	Gaining unauthorized access to ground station systems.	Compromising accounts, exploiting insecure remote access, unauthorized control of satellite operations.
Data Manipulation Attacks, Sec. IV-C2	Tampering, Information Disclosure	Unauthorized alterations to data transmitted by ground stations.	Manipulating satellite commands, telemetry data, and introducing malware.
Software Attacks and Zero-Day Exploits, Sec. IV-C3	Tampering, Information Disclosure, Elevation of Privilege	Exploiting software vulnerabilities in GSs systems.	Exploiting unpatched or outdated software, zero-day exploits, and firmware manipulation.
Denial of Service Attacks, Sec. IV-C4	DoS	Overwhelming networks with traffic to disrupt satellite links.	Impacting availability, unique vulnerabilities in Satcoms.
Netw. + Cloud-Based Attacks, Sec. IV-C5	Spoofing, Elevation of Privilege,DoS	Exploiting network vulnerabilities for unauthorized access.	Social engineering, exploiting network vulnerabilities, unauthorized software use.
Cyberattacks on Satcoms Links Segment, Sec. IV-D			
Link Jamming, Sec. IV-D1	DoS, Tampering	Flooding communication channels with RF interference.	Disrupts availability and tampers with signal integrity.
Links Eavesdropping, Sec. IV-D2	Information Disclosure	Intercepting and listening to data transmitted via RF signals.	Accessing data and potentially exploiting it for intelligence purposes.
Signal Spoofing, Sec. IV-D3	Spoofing	Illicit manipulation of signals to deceive receivers.	Generating spoofing (deceive receiver) and forwarding spoofing (delay signal).
Signal Hijacking, Sec. IV-D4	Spoofing, Elevation of Privilege	Unauthorized access and control over Satcoms signals.	Unauthorized use of Satcoms for signal transmission or manipulation.
Cyberattack Vectors on Overall Satcoms Systems, Sec. IV-E			
Cognitive Radio-based Attacks, Sec. IV-E1	Spoofing, DoS, Elevation of Privilege, Repudiation	Exploits cognitive radio technology for unauthorized access, spoofing, DoS, and privilege escalation.	Unauthorized access, frequency hopping, mimicry, privilege escalation.
Satel. Spoof., Replay Attacks, Sec. IV-E2	Spoofing, Repudiation	Falsification of satellite signals and data, creating repudiation threats.	Falsification of satellite signals, replaying intercepted signals.
Unauthorized Satellite Commanding, Sec. IV-E3	Tampering, Elevation of Privilege	Unauthorized access to satellite control systems, tampering with commands, and privilege escalation.	Unauthorized access, command manipulation, elevated privileges.
Satellite Constel. Vulnerab., Sec. IV-E4	Tampering, DoS	Attacks targeting satellite constellations, leading to tampering and DoS threats.	Tampering with interconnected satellites, disrupting satellite constellation.
Protocol Exploitation and Layer-specific Attacks, Sec. IV-E5	Tampering, Information Disclosure, DoS, Elevation of Privilege	Attacks targeting different protocol stack layers (physical, transport, presentation) for various purposes.	Session hijacking, data packet manipulation, encryption weaknesses.
Cross-Segment Chain Attacks, Sec. IV-E6	Tampering, DoS, Elevation of Privilege	Simultan. tampering of ground and space segments, leading to system-wide threats.	Tampering with both segments, disrupting communication, privilege escalation.
System-wide Supply Chain Attacks, Sec. IV-E7	Spoofing, Tampering, Repud., Info. Discl., DoS, Elev. of Privil.	Attacks exploiting the supply chain to introduce vulnerabilities and compromise the entire Satcoms system.	Spoofing, tampering during production, information theft, DoS, privilege escalation.

[110], [134], [135]. The STRIDE model [134] classifies attacks into Spoofing [143], [70], Tampering [110], Repudiation [106], Information disclosure [105], DoS [137], and Elevation of privilege [69], [110] attacks, as summarized in Table VI. The STRIDE model can be seamlessly integrated with other methodologies, such as the Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD) model [132], [135] and Attack Trees [144], to enhance the scope of the threat analysis [110].

We note that not all classifications of the STRIDE model may be applicable to each Satcoms segment (space, ground, links) in the same manner. Additionally, a single Satcoms-specific cyberattack category at a particular Satcoms segment can fall into multiple classifications in the STRIDE model,

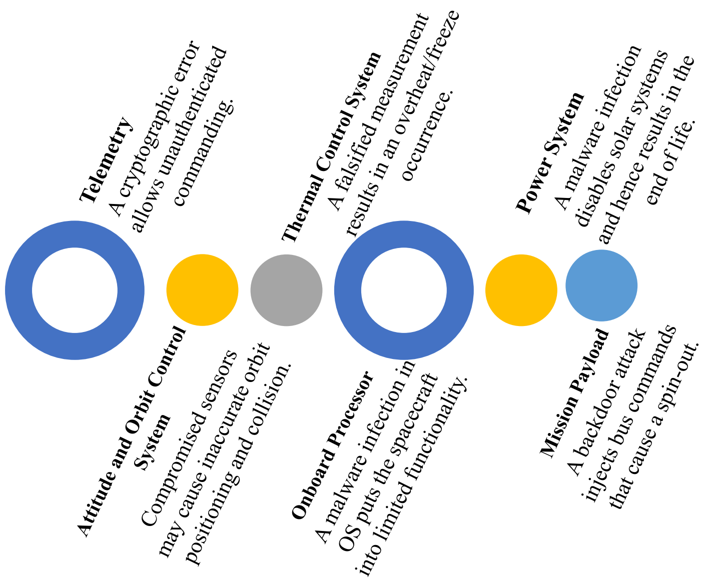

Telemetry
A cryptographic error allows unauthenticated commanding.
Thermal Control System
A falsified measurement results in an overheat/freeze occurrence.
Power System
A malware infection disables solar systems and hence results in the end of life.
Attitude and Orbit Control System
Compromised sensors may cause inaccurate orbit positioning and collision.
Onboard Processor
A malware infection in OS puts the spacecraft into limited functionality.
Mission Payload
A backdoor attack injects bus commands that cause a spin-out.

Fig. 9. Summary of cyberattacks on space segment: Examples of potential attacks on onboard subsystems of a satellite.

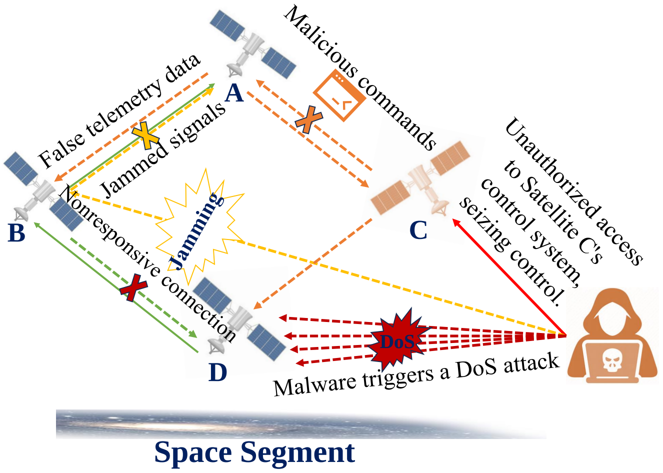


Fig. 10. Illustration of cyberattacks on space segment: Potential cyberattacks on broader satellite-to-satellite space segment of Satcoms system.

see Table VII. For instance, the satellite hijacking and control takeover attack category (see Section IV-B2) falls into the spoofing and elevation of privilege classifications in the STRIDE model. Therefore, we did not adopt the classifications of the STRIDE model as the main organization scheme for the cyberattacks in a given Satcoms segment. Rather, we created a novel comprehensive categorization of the Satcoms-specific cyberattacks. This novel organization scheme allows us to pursue a Satcoms attacks-focused perspective while acknowledging the multifaceted nature of the Satcoms cyberattacks, which often fall into multiple classifications of the general STRIDE model. Essentially, our organization scheme aligns our survey categorizations with the existing real-world security issues that are specific to Satcoms, while allowing for linkages of our Satcoms-specific cyberattack categories with the threat classifications in the general STRIDE model.

B. *Cyberattacks on Space Segment*

While satellites in orbit have limited direct physical interactions with individuals, they are still susceptible to cybersecurity threats [143]. The space segment, which includes the satellites and their onboard subsystems, can face various vulnerabilities that may lead to compromised functionalities and security controls [36]. Figure 9 illustrates potential attack scenarios on the onboard subsystems of a given satellite that could result in mission failure.

Beyond a satellite's onboard subsystems, the broader satellite-to-satellite space segment of Satcoms systems is also vulnerable to significant cyberthreats, as illustrated in Figure 10. These cyberthreats encompass satellite hardware and software threats, hijacking and control takeover, signal jamming and interference, as well as data injection and manipulation.

Figure 10 illustrates a scenario where multiple satellites (A, B, C, D) are interconnected for global communication; whereby, Satellite A functions as a central hub, relaying data between satellites. In this satellite-to-satellite communication context, examples of cyberattacks include the following: Satellite C's control is hijacked [145], [146], leading to malicious commands disrupting Satellite A's data relay. Satellite B faces signal jamming [147], severing its connection with Satellite A. Satellite D is compromised with malware [148], causing a communication blackout; and false telemetry data that is injected into Satellite A distorts the decision-making across network. These exemplary attacks illustrate the vulnerabilities in the broader satellite-to-satellite system, emphasizing the need for robust countermeasures to safeguard against these threats [44].

1) *Hardware and Software Attacks:*

The space segment of Satcoms systems is susceptible to cyberattacks that specifically target the hardware and software components of satellites [28], [24]. These attacks can be classified under the tampering, information disclosure, and elevation of privilege threat classifications in the STRIDE model [110]. As a result of such attacks, there is a risk of compromising the confidentiality, integrity, and availability of Satcoms communication links [12].

Cybercriminals may employ diverse techniques, including the use of malware [148], DoS attacks [36], and other cyberthreats, to achieve their malicious objectives [24]. Through these methods, they can disrupt communication channels, manipulate critical data, or even attempt to steal sensitive information from satellites [12], [36]. Thereby, it should be noted that malware and DoS attacks are software-based attacks that can also target hardware components and disrupt satellite systems.

Furthermore, the use of cost-effective and readily available Commercial Off-The-Shelf (COTS) hardware and software in space infrastructures can introduce new vulnerabilities [149]. The integration of COTS components may not undergo rigorous cybersecurity assessments, potentially leaving space systems susceptible to exploitation [111]. As the demand for cost-efficient space solutions grows, the adoption of COTS hardware and software components becomes more prevalent, making it imperative to address the associated cybersecurity risks to safeguard the space segment [16].

The space segment is also susceptible to malfunctions caused by hardware or software failures [84]. Hardware defects, software bugs, or operational errors can lead to satellite anomalies or complete system failures, disrupting the functionalities and communication capabilities of the satellite [150]. Such malfunctions may result in the satellite ceasing to function correctly or providing inaccurate data, potentially leading to severe communication disruptions and the inability to fulfill the satellite's intended mission objectives [24].

Moreover, the space segment can be at risk from unpatched or outdated software, leaving it vulnerable to exploitation by cybercriminals [16]. As the threat landscape evolves, patches and updates must be regularly applied to the onboard components of space systems to address newly discovered vulnerabilities and enhance the overall cybersecurity posture [36]. Regular software maintenance and timely application of security patches are crucial to safeguard the space segment against potential cyberattacks [69].

We note that the hardware and software attacks may straddle both the category of attacks on an individual satellite's onboard systems (see Figure 9) as well as the broader satellite-to-satellite space segment (see Figure 10). For example, an attack on an individual satellite's software (onboard) could be part of a broader strategy to compromise the satellite-to-satellite communication network. In such cases, the hardware and software attacks apply to both contexts, underscoring their relevance to both the individual satellite (onboard) and the broader space segment.

2) Satellite Hijacking and Control Takeover: Satellite hijacking is a highly concerning cyberattack that falls under the spoofing [143], [70] and elevation of privilege threat classifications of the STRIDE model [110]. Through satellite hijacking, cybercriminals attempt to gain unauthorized control over a satellite, allowing them to manipulate the functions and operations of the satellite [145], [146]. Satellite hijacking attacks typically target vulnerabilities in the satellite's communication protocols [6], command interfaces [124], or onboard software [84]; commonly, the attacks attempt to exploit these vulnerabilities using sophisticated spoofing techniques [143], [70].

Spoofing is the ability to intercept, modify, and re-transmit a communication stream to deceive the recipient [44]. Spoofing allows attackers to seize control of the satellite by impersonating a legitimate communication source, thereby tricking the satellite's systems into accepting unauthorized commands [147]. Once recognized as a legitimate entity, fraudulent commands can be injected into the satellite's command receiver, leading to malfunctions or mission failures [24].

The consequences of a successful satellite hijacking can be severe and far-reaching [69]. By gaining control of the satellite, attackers can manipulate its orbit, disrupting its intended trajectory and thereby potentially causing collisions with other satellites or space debris [29]. This hijacking scenario can set off a chain reaction affecting space operations, including Satcoms, Earth observation, and navigation systems [145], [146]. Furthermore, satellite hijacking empowers attackers to interfere with communication services, impacting industries reliant on satellite-based communication. This includes emergency services, military operations, global internet connectivity, and disaster response [147].

Moreover, the capability to manipulate a hijacked satellite transforms the satellite into a potent weapon, which could be directed against other space assets or even targeted towards Earth [145], [146]. This raises concerns about potential physical or cyber-kinetic attacks [28] originating from space, posing significant risks to national security and the global space infrastructure [151].

3) Satellite Signal Jamming and Interference: Signal jamming [147], [28] deliberately floods communication channels with high-power interference signals, effectively initiating a DoS attack [16] in the STRIDE model classification [110]. The signal jamming aims to sever legitimate communication links between satellites and GSs or even to disrupt communication between satellites themselves [36].

The impact of a satellite signal jamming attack can be devastating, affecting critical applications that heavily rely on uninterrupted satellite connectivity [107]. During crises and disasters, emergency services heavily depend on seamless communication to coordinate response efforts and to ensure public safety [16], [143]. However, jammed communication channels cannot effectively relay vital information, delaying emergency services and potentially jeopardizing lives [36], [60].

Similarly, military operations heavily rely on secure and reliable communications for command and control capabilities [152]. An interference-induced communication outage can impede real-time information exchanges among military units, leading to disruptions in operations, reduced situational awareness, and compromised mission success [49], [24].

Furthermore, navigation systems, including GPS, are integral to a wide range of industries, including aviation, maritime shipping, transportation, and precision agriculture [54]. Jamming these navigation signals can lead to navigation errors, resulting in accidents, disruptions in supply chains, and significant financial losses for businesses [16], [153]. Thus, while the primary goal of signal jamming is to deny service by flooding communication channels with interference signals, there can be secondary effects involving tampering with the data being transmitted, depending on the attacker's objectives [6].

4) Data Injection and Manipulation: Within the space segment of Satcoms systems, a significant cybersecurity concern is data injection and manipulation, falling under the threat classifications tampering and information disclosure in the STRIDE model [110]. This insidious threat exploits vulnerabilities in satellite data links to inject malicious data, resulting in data manipulation and the transmission of false information [16]. The consequences of data injection and manipulation attacks can be severe, particularly in scenarios involving spacecraft maneuvers or space missions [49].

Data manipulation poses significant risks to the integrity and reliability of Satcoms systems [105]. By injecting false information into the data transmission, attackers can mislead ground controllers, satellite operators, or other spacecraft in the network, potentially leading to critical errors in decision-making processes [49]. For instance, falsified telemetry data could misguide engineers in assessing the satellite's health and performance, leading to incorrect diagnostics and ineffective troubleshooting efforts [154].

Furthermore, attackers may aim to cause potential misinformation by altering the data sent from the satellite to GSs [49]. This misinformation can have detrimental effects on various sectors relying on satellite data, such as weather forecasting, environmental monitoring, and scientific research [16], [155]. The dissemination of inaccurate data can lead to incorrect predictions, hampering disaster response efforts, and disrupting climate monitoring and agricultural planning [155].

Data manipulation attacks also open doors to unauthorized access to sensitive information transmitted via satellite data links [49]. Malicious actors may exploit these vulnerabilities to intercept and exfiltrate sensitive data, compromising the confidentiality of critical communications and potentially resulting in data breaches [107].

In space missions, where precision and accuracy are paramount, data manipulation attacks can lead to catastrophic consequences [24]. By sending altered commands to spacecraft, attackers could disrupt maneuvers, change orbital trajectories, or compromise critical systems [6]. Such interference could lead to mission failure, satellite collisions, or the creation of dangerous space debris, posing risks to other satellites and future space missions [24], [49].

In conclusion, data injection and manipulation represent a multifaceted threat that extends from Satcoms systems to broader sectors reliant on satellite data, emphasizing the pressing need for robust cybersecurity measures to safeguard both space operations and terrestrial applications.

C. Cyberattacks on Satcoms Ground Segment

Generally, the easiest way to control a satellite, and subsequently the Satcoms system, is to compromise the ground segment since the ground segment already has the tools and software to legitimately control and track the satellite [156]. Also, tried-and-true terrestrial attacks [16], [125] can be directed at the ground segment. Attackers targeting the ground segment can exploit vulnerabilities to illicitly gain access and control. They can execute various attacks, including unauthorized access, data manipulation, DoS attacks, software attacks, and cloud-based attacks [157].

1) Unauthorized Access and Control: Attackers may attempt to gain unauthorized access to GSs, which falls under the elevation of privilege threat classification in the STRIDE model [110]. By compromising administrative or operator accounts, cybercriminals can manipulate satellite control systems and execute unauthorized commands [147]. This can lead to the alteration of satellite configurations, unauthorized maneuvers, or the initiation of hazardous commands [24].

Moreover, attackers can exploit insecure remote access mechanisms or unpatched software in GSs systems, enabling the attackers to take control of satellite operations [157]. This unauthorized control can disrupt Satcoms, interfere with mission-critical operations, and compromise the security of satellite networks [24].

2) Data Manipulation Attacks: Data modification attacks pose a serious threat to GSs and the overall integrity of Satcoms systems [155]. These attacks, which fall into the tampering and data disclosure classifications of the STRIDE model [110], involve unauthorized alterations of data transmitted or stored by GSs. Additionally, data modifications can occur intentionally or accidentally due to technical errors or glitches in GS operations [16]. One of the primary objectives of data modification attacks is to manipulate the information being communicated between GSs and satellites. For example, an attacker may modify satellite commands sent from the GS to the satellite, leading to incorrect or malicious instructions being executed by the satellite's onboard systems. Such altered commands could cause the satellite to deviate from its intended trajectory, disable critical subsystems, or perform unauthorized actions [35]. This could lead to mission failure, communication disruption, or even the loss of the satellite [16], [24].

Moreover, data modification attacks can target the telemetry data transmitted from the satellite to the GS. Telemetry data includes vital information about the satellite's health, status, and performance [154]. By altering this data, attackers can potentially hide system malfunctions, present false readings, or disrupt the GS's ability to accurately monitor the satellite's condition [16]. Consequently, GS operators may be unable to identify critical issues, leading to delayed responses to anomalies, and consequently, increased risk of satellite failure [155].

Another concern with data modification attacks is the potential for unauthorized software use [35]. Attackers may inject malicious software or malware into the GS's data stream, and if undetected, this malware can infiltrate the satellite's onboard systems during data processing [148]. This could enable attackers to gain unauthorized access and control over the satellite, compromising its operations and allowing the attacker to execute further attacks [35].

Data manipulation in the context of Satcoms can also compromise sensitive information. Satcoms systems handle various types of data, including communication traffic, mission-critical information, and user data [105]. Attackers may modify this data to gain unauthorized access to confidential information, steal sensitive data, or manipulate communications to their advantage [24].

3) Software Attacks and Zero-Day Exploits: Software attacks and zero-day exploits in the ground segment of Satcoms systems fall primarily under the tampering classification in the STRIDE model [110]. Depending on the specific nature of the attack [6], they can also have implications for the information disclosure and elevation of privilege attack classifications.

Software vulnerabilities pose a significant risk to the ground segment of Satcoms, just like any other computer system [35]. Attackers often target unpatched or outdated software running on GSs to exploit known vulnerabilities, engaging in activities that primarily fall under tampering in the STRIDE model [16]. The deployed software must constantly be updated with the most recent version, which includes the fixes for the found vulnerabilities [118]. Failure to apply patches leaves applications susceptible to attack, as attackers can exploit these known weaknesses, gaining unauthorized access or disrupting GS operations [69]. In some instances, software attacks and zero-day exploits can lead to information disclosure [110]. Attackers may exploit vulnerabilities to gain unauthorized access to sensitive data stored within the ground segment. This could include confidential communication data, user credentials, or other critical information, thereby compromising the confidentiality of the system [6].

Additionally, these attacks can result in the elevation of privilege [110]. Attackers with in-depth knowledge of satellite software and firmware may attempt firmware manipulation attacks [158], [140], [141]. By compromising the firmware of GSs equipment, attackers can introduce malicious code that operates at a low level and can persistently control various aspects of satellite operations. Such firmware attacks can result in the manipulation of satellite commands, unauthorized access, and even the deployment of hidden functionalities. Firmware manipulation attacks can be extremely challenging to detect and mitigate, as they occur at a level that is often less monitored than higher-level software components [36], [155], [140], [141].

Overall, zero-day exploits present a formidable threat to the Satcoms ground segment [35]. These zero-day attacks exploit previously unknown vulnerabilities in hardware or software, for which no patches or defenses exist at the time of discovery [16]. Attackers can take advantage of these undiscovered weaknesses to breach security measures before mitigations are developed and deployed [35]. The presence of zero-day exploits in the GS infrastructure can be leveraged for advanced persistent threats (APTs) [159], allowing attackers to maintain prolonged, undetected access, and potentially leading to severe consequences, such as data theft, sabotage, or espionage [118].

4) Denial of Service (DoS) Attacks: DoS and Distributed DoS (DDoS) attacks pose significant threats to the Satcoms ground segment. These highly disruptive cyberattacks aim to incapacitate a network or system by overwhelming it with an extraordinary volume of traffic, rendering it unreachable to legitimate users [44], [137]. While the general concept of DoS and DDoS attacks is broad, understanding their specific implications for the Satcoms ground segment is crucial [137].

Within the Satcoms domain, there exist distinct vulnerabilities associated with DoS attacks on ground segments [157]. One such distinct vulnerability is the reliance on a limited number of Ground Stations (GSs) for communication with satellites [123], [125], whereby each of the few GSs supports a relatively large terrestrial network with numerous end users. Attackers can exploit this by overwhelming these few GSs with a high volume of traffic, disrupting satellite links, and causing service interruptions. Additionally, the easy accessibility of the ground segment can make it susceptible to jamming attacks, where malicious actors transmit interference signals to disrupt or block satellite signals [153], [20]. These unique vulnerabilities inherent to the Satcoms ground segment intensify the potential impact of DoS attacks, making the DoS attacks particularly concerning for organizations relying on satellite systems for critical operations [114], [160].

Moreover, DDoS attacks present a heightened risk in Satcoms domain due to their massive scale and distributed nature [137], [161], [162], [163], [164]. In a DDoS attack, hackers leverage a multitude of hijacked or compromised devices, e.g., ordinary computers and IoT devices in the GSs, to amplify the attack's impact [114]. This amplification effect magnifies the volume of the attack traffic that impacts the limited number of GSs, significantly complicating mitigation efforts [17], [114], [165], [166], [167]. Detecting the origins of the attack and filtering out malicious traffic amid legitimate requests becomes a formidable challenge [137].

A successful DoS or DDoS attack on a Satcoms ground segment can result in severe financial losses, reputational damage, and operational disruptions [114]. The loss of satellite connectivity can impact vital operations, such as emergency services, military operations, aviation, and maritime navigation [98], [99], [137].

5) Network and Cloud-Based Attacks: The ground segment's connection to terrestrial computer networks introduces a potential avenue for cyberattacks on Satcoms. Cyber attackers can exploit vulnerabilities within these terrestrial networks to gain unauthorized access to GSs, introducing threats such as spoofing, elevation of privilege, and DoS based on the STRIDE model [110]. Social engineering attacks, including phishing, can be utilized to deceive GS operators, leading to the disclosure of sensitive information or unauthorized access [69]. Additionally, attackers may leverage known vulnerabilities in network technologies to infiltrate GS networks and execute malicious activities [168]. Once within the GS network, cyber adversaries can focus on manipulating satellite commands and telemetry data. Tampering with satellite commands may result in unauthorized actions, potentially causing satellites to deviate from their intended orbits or perform harmful maneuvers. Such actions can disrupt communication services, jeopardize satellite integrity, and even lead to satellite loss [69].

Furthermore, attackers may extract sensitive information from the GS network. This sensitive information may encompass proprietary Satcoms protocols, confidential user data, or critical operational information. Unauthorized access to such data may furnish valuable intelligence for future attacks or be exploited for malicious purposes, presenting substantial risks to the overall security of Satcoms systems [168].

Recently, the adoption of cloud-based solutions by GSs has surged, driven by demands for scalability and cost efficiency [169]. While cloud infrastructures offer an efficient platform for storing, processing, and analyzing large volumes of satellite data [170], this shift also introduces new cybersecurity challenges and potential vulnerabilities, particularly in the context of Satcoms.

A primary concern for cloud-based GSs is the susceptibility to DDoS attacks. Attackers may target cloud service providers hosting GSs with a deluge of traffic, overwhelming resources, and causing service disruptions [36]. A GS falling victim to a DDoS attack could become unreachable, impeding crucial communication between the GS and the satellite. Such disruptions can have severe implications, including mission delays, service outages, or compromised satellite operations [36], [24].

Additionally, cloud service providers themselves may en-

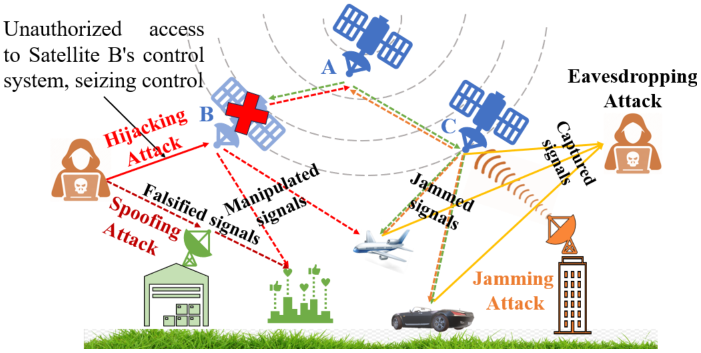
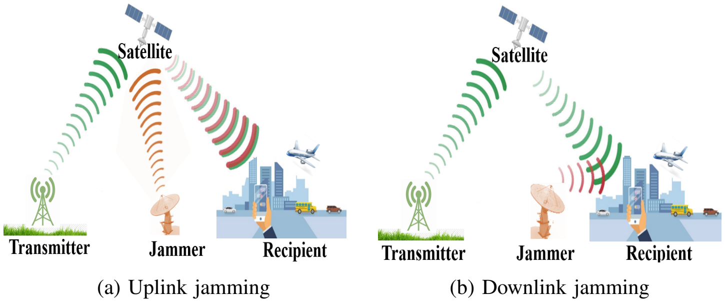


Fig. 11. Illustration of potential cyberattacks on links segment of Satcoms system.



(a) Uplink jamming

(b) Downlink jamming

Fig. 12. Illustration of different types of jamming.

counter security breaches or vulnerabilities, potentially exposing GSs to additional risks [171]. In such scenarios, attackers might gain unauthorized access to GS data, compromise sensitive information stored in the cloud, or exploit cloud infrastructures to launch further attacks on the GS or other critical systems [16], [171].

D. Cyberattacks on Satcoms Links Segment

The links segment of Satcoms plays a crucial role in facilitating communication with satellites, typically achieved through the transmission of RF waves, often within the GHz range [17], see Section III-A. During a satellite's operational lifespan, there is an inherent risk of compromise to its TT&C functions and data communications. Malicious actors may seek to exploit vulnerabilities within the ground segment; thereby, affecting the links segment of the Satcoms systems. Therefore, affected parties may need to gather additional information to identify the nature and scope of the attack, and to implement countermeasures to mitigate its effects [6]. Additionally, they may need to increase their monitoring and detection capabilities to prevent future attacks. This section surveys the attack techniques that can be used to obstruct the data communications on Satcoms links.

Figure 11 illustrates several cyberattacks on the Satcoms links segment in the context of a network with Satellite A operating as a central hub of the Satcoms network. Signal eavesdropping [16] is illustrated for an attacker that seeks to compromise the communication signals traveling to and from Satellite C. Simultaneously, a signal-jamming attack [44], [153] is launched at Satellite C, aiming to disrupt these signals. This combined attack not only jeopardizes the integrity of the communication but also severs Satellite C's connection with Satellite A. This disruption significantly impacts the data relay process between Satellites A and B, extending the repercussions of the attack to the connected ground-based units, including buildings, cars, and airplanes.

Furthermore, with a signal hijacking attack [147], [145], [146], an attacker manages to gain unauthorized control over the signals originating from Satellite B. This signal hijacking results in the transmission of malicious commands that disrupt both Satellites A and B, further affecting the ground-based units, including buildings and airplanes. The compromised signals lead to chaos and potentially critical failures within the system. Furthermore, with a sophisticated signal spoofing attack [28], the attacker introduces falsified signals into the communication network. These deceitful signals are directed towards the ground-based components.

These exemplary attacks are reminders of the vulnerabilities within the link segment of the Satcoms system [15], [139], [17]. They underscore the critical necessity for the implementation of robust countermeasures to fortify the system against these multifaceted threats [44]. The interconnected nature of these attacks showcases the potential cascading effects, emphasizing the urgency of safeguarding Satcoms systems against such complex and coordinated threats [114], [172].

1) Link Jamming: The link jamming cyberattack falls within the DoS and tampering classifications of the STRIDE model [110]. Link jamming directly aligns with the DoS classification, as link jamming aims to flood a targeted communication channel with powerful RF signals [44]. This flooding overwhelms the channel and prevents legitimate communication from taking place. In essence, link jamming obstructs reliable and uninterrupted communication between satellites and GSs. This link jamming attack disrupts the availability of the communication channel, rendering the channel unusable for its intended purpose [153]. While the primary objective of link jamming is to disrupt communication (i.e., a DoS attack), link jamming also involves tampering with the integrity of the communication signals. Attackers utilize jammers emitting noise-like signals to tamper with or alter the desired signals' integrity [153], [174]. By tampering with the signals, they effectively block the reception of legitimate data by introducing unwanted noise into the communication channel [17]. This tampering compromises the integrity of the transmitted data [106], [105].

The jammers can focus on either the uplink, which refers to communication signals sent from GSs to satellites, or the downlink, which pertains to signals transmitted from satellites to GSs [16], as exemplified in Table VIII and illustrated in Figure 12. The jammer is made up of two distinct groups of receivers: primary and secondary [16]. Four channelized and four cued receivers make up the primary receiver group. They work together to achieve immediate signal capture, precise parameter measurement, quick updates, and accurate geolocation [44]. This is done by using GPS tracking or a device's Internet Protocol (IP) address as a geolocation mechanism [173]. The secondary receiver group, in turn, offers a wider range of

TABLE VIII: Jamming classifications.

Specification	Uplink Jamming	Downlink Jamming
Impact	Low impact due to increased satellite autonomy.	More impact.
Difficulty	More difficult.	Much easier.
Effect	Global.	Local.
Signals	Payload signals and command uplinks.	Communication or navigation signals.
Targets	The radios' sensors and command receivers on the satellites.	Satcoms and Navigation Satellite (NAVSAT) broadcasts, and ground-based receivers for satellite data.
Requirements	Significant jammer transmitter power.	Only a very low-power jammer.
Technologies	Based on official Signals Intelligence (SIGINT) or Open Source Intelligence (OSINT) [173].	Cutting-edge technologies are emerging, including a handheld GPS jamming system sold by Russia [147].
Effectiveness	The effectiveness of jamming is heavily reliant on obtaining detailed information about the target signal.	Contingent upon the jammer's capacity to function within the ground site's Line-of-Sight (LoS), the antenna's field of view, and the processing of the jamming signal by the Satcoms receiver. Also, evaluating its effectiveness can be challenging since it usually necessitates monitoring the output of the targeted receiver, which is frequently unfeasible [28].

frequencies, takes the place of the primary one in long-term measurements, contributes to the identification of intra-pulse modulation, and updates geolocation estimations [173].

Both uplink and downlink jamming are threats to all commercial and military Satcoms systems [17]. In either scenario, the jammer needs to use the same radio band as the system it is intended to disrupt. Ground-based uplink jammers must have nearly the same power as the ground-based emitter connected to the link being jammed [147]. Downlink jammers that are based on the ground, however, can frequently be far less powerful and still be effective [44]. Attacks on a satellite's uplink during crucial commanding times may significantly reduce mission performance as most satellites depend on uplinked Command and Control (C2) information from the GSs for maintenance, payload control, and satellite health and condition [173]. However, due to limited Line-of-Sight (LoS) [147] and growing satellite autonomy, the effectiveness of uplink jamming is constrained. As a result, downlink jamming attacks are frequently easier and more effective [175].

For over 30 years, commercial Satcoms have been the target of deliberate jamming [34], [152]. In one of the early instances, a man intercepted, jammed, and substituted his own message for the Home Box Office (HBO) satellite broadcast in 1986 using equipment that was readily available [176]. Commercial providers have resisted making changes to their Satcoms to handle intentional jamming, as opposed to unintentional interference, for most of the last 30 years, claiming high costs or merely hoping that jamming occurrences will decrease. In fact, there are more jamming incidents currently than ever before, particularly in the Middle East as a result of the Arab Spring and the upheaval in Iran [177]. The Arab Spring-related interference has reportedly reached a point where it is materially affecting the revenue of two businesses, Arabsat and Nilesat [176]. Due to an increase in deliberate interference in the Middle East, commercial satellite fleet operator Eutelsat [153] revealed in 2013 that it was installing an experimental anti-jamming technology on one of its forthcoming satellites.

2) Links Eavesdropping: Data transmitted over a communication channel can be intercepted by links eavesdropping [16], [142] which falls into the information disclosure classification of the STRIDE model [110]. Since all communications for satellite and ground systems are sent as RF signals over the air, they are all vulnerable to interception [49]. Sometimes, information sent over RF signals is not encrypted or has only weak encryption that can be cracked to reveal the plain text. Furthermore, data encryption for Satcoms has a number of drawbacks [44], [49], [88], including increased operational costs and reduced overall performance. These factors often preclude commercial satellite operators from using encryption and, of course, attract attackers [34], [152].

One of the tools used by security services in many nations to eavesdrop on data transmitted over the air is Signals Intelligence (SIGINT) [176]. Eavesdropping is a form of SIGINT that intercepts and listens in on communications between two parties. Through eavesdropping, data transmitted via satellite or another method can be accessed and potentially exploited for intelligence purposes [49]. Historically, only governments and specialized individuals had the capability to eavesdrop on Satcoms. However, we found numerous publicly accessible examples of eavesdropping tools that are either available commercially or that users can create on their own with little expense and technical skill [149].

One instance of satellite eavesdropping occurred in 2009 when hackers in Iraq used the $26 Russian SkyGrabber tool [175] to record video feeds from the United States military Predator Unmanned Aerial Vehicles (UAVs) [178]. Through commercial Satcoms, insurgents eavesdropped on the unencrypted video feed that was returned from UAVs. Unfortunately, several commercial satellite systems still suffer from these encryption flaws [176]. Thus, non-governmental traffic passing through those networks may still be exposed. The government solves this problem by requiring encryption for military communications that rely on commercial platforms [17], [152]. Although eavesdropping is a passive method of signal exploitation [67], commercial providers are also impacted by other, more active types of interference, as surveyed next.

3) Signal Spoofing: Signal spoofing, which falls under the spoofing threat classification in the STRIDE model, is among the most intricate and covert methods employed for targeting Satcoms [28]. Recently, the study [179] investigated the cybersecurity aspects of COSPAS-SARSAT satellite-based systems, which serve as an international search and rescue program by utilizing satellite-aided tracking systems to provide timely and precise distress alerts and location data. The study [179] demonstrated the first successful attacks on COSPAS-SARSAT protocols, including replay and spoofing activities.

The two main types of spoofing attacks are generating spoofing attacks and forwarding spoofing attacks [147]. In the generating spoofing attack, the receiver is directed to capture and track the spoofing signal subconsciously as a result of the spoofer's autonomous Satcoms signal generation and transmission. The receiver then produces incorrect information as a result of this type of spoofing, which gradually leads the receiver away from the proper responses [147]. Such a spoofing attack is referred to as the spoofing process of the generating spoofing attack.

In contrast, a forwarding spoofing attack is easier to conduct than a generating spoofing attack [1]72. In the forwarding spoofing attack, the spoofer intercepts the real signal that the satellite is sending to the receiver and delays it before sending it to the target receiver. Except for the delay and amplitude, the interference signal is therefore identical to the real signal. To increase the likelihood that their attacks will succeed, forwarding spoofing attacks must use interference techniques that are consistent with such attacks [180].

These advanced spoofing strategies introduce a layer of complexity and sophistication to Satcoms attacks, posing a significant challenge to the integrity and security of communication systems that rely on satellite technologies [28].

4) Signal Hijacking: Signal hijacking is the illicit use of a Satcoms system for the transmission of a particular signal; or for taking over the control of a signal, such as a broadcast signal, and replacing it with another [178]. Specifically, Satcoms signal hijacking entails the unauthorized access or control of Satcoms by a third party. Signal hijacking attacks can be carried out by various means in Satcoms systems, including by hacking into the ground control systems, compromising the satellite itself, or intercepting and manipulating the satellite's communication signals [147]. Satcoms signal hijacking attacks fall mainly into the spoofing and elevation of privilege classifications of the STRIDE model [110].

Once a Satcoms signal hijacking has occurred, the attacker can use the system to intercept or manipulate communications between other users, disrupt the normal functioning of the system, or launch further attacks against other targets [147]. For example, an attacker could use a hijacked Satcoms system to eavesdrop on sensitive military or government communications, interfere with air traffic control systems, or disrupt the operations of commercial satellites or ground-based networks [36]. A signal hijacking attack can be particularly difficult to detect and defend against, as these attacks often involve sophisticated techniques and can be carried out from remote locations. Recent incidents of Satcoms signal hijacking include:

- In 2007, the Tamil Tigers in Sri Lanka used Intelsat satellites to transmit propaganda [181].
- In 2009, Brazilian authorities apprehended several civilians who configured homemade equipment to utilize the frequencies reserved for the Satcoms system of the United States Navy's fleet for their private communications [181]. Also, 2009 saw the discovery of security vulnerabilities in Satcoms technologies that enabled attackers to access Command and Control (C2) systems and commit data breaches. Russian attackers who may have been underpinned by the government were thought to have exploited these vulnerabilities as early as 2007 [182].
- In 2013, hackers broadcast a report of a zombie invasion through the emergency alert systems of TV stations in Montana and Michigan [183]. It is ambiguous whether a satellite attack or an Internet connection allowed for the illicit transmissions. Many security experts thought that a satellite attack was more likely because of the reports' lack of specificity.
- In 2015, a security researcher demonstrated that for $1,000, anyone could create a system capable of sending fake data to a GlobalStar satellite. GlobalStar is a system that monitors critical industrial infrastructure, such as pipelines, as well as tracks hikers and other adventurers who use GlobalStar's consumer tracker [176].

E. Cyberattack Vectors on Overall Satcoms Systems

In addition to the cyberattack vectors on the individual segments of Satcoms systems (space segment, ground segment, and links segment) that have been surveyed in Sections IV-B– IV-D, there are broader attack vectors that can target the overall Satcoms infrastructure. These broader attack vectors exploit weaknesses or vulnerabilities that exist across the entire Satcoms ecosystem, potentially leading to severe consequences [16]. This section comprehensively surveys the broad cyberattack vectors on overall Satcoms systems.

1) Cognitive Radio-based Attacks: Cognitive radio technology, which enables devices to dynamically adapt their operating parameters based on environmental conditions, introduces both opportunities and vulnerabilities within the Satcoms system [184]. While the cognitive radio technology increases the spectrum efficiency [41], [185], it renders the overall system vulnerable to a range of threats, including spoofing, DoS, and elevation of privilege [184].

Attackers can exploit cognitive radios to gain unauthorized access to Satcoms frequency bands [44]. By manipulating the cognitive radio's configuration, attackers can mimic legitimate users, deceiving Satcoms systems into granting them access. This spoofing activity can disrupt communications, introduce malicious actors into the network, and compromise the integrity of the Satcoms services. Cognitive radios can also be employed to execute DoS attacks. Attackers may utilize frequency-hopping techniques [186] to rapidly switch frequencies or to manipulate cognitive radios to interfere with legitimate communications. This frequency-hopping evasion can make it challenging to detect and mitigate the attack, resulting in disrupted and unreliable Satcoms services [41].

Attackers who gain unauthorized access to Satcoms frequency bands through cognitive radio manipulation can potentially escalate their privileges within the network [44]. These elevated privileges can provide them with greater control over Satcoms communications, posing significant security risks [24].

Furthermore, cognitive radio-based attacks exacerbate the attribution problem, a key challenge confronting space asset organizations in responding to cyberattacks [19], [24]. Satellites rely on networks, including the internet, where data transmissions are divided into packets that take independent, packet-switched routes to their destination [187]. This complexity in data routing makes it difficult to trace the source of a cyberattack, offering attackers a high degree of deniability [110]. Cyberattacks leveraging cognitive radio technology can exploit this attribution challenge, making them an attractive means to disrupt and harm space systems while leaving little evidence of their origin [184].

2) Satellite Spoofing and Replay Attacks: The overall Satcoms systems are highly vulnerable to spoofing and replay attacks, in conjunction with repudiation threats [28], [24]. Spoofing and replay attacks falsify the satellite signals and location information, which can have far-reaching consequences for the Satcoms ecosystem [179], [117]. The relation between spoofing/replay attacks and repudiation threats lies in the potential for attackers to use spoofing techniques to manipulate data or communication in a way that allows them to later repudiate their actions. For example, in a Satcoms system, an attacker may spoof the source of a command to a satellite, making it appear as if the command came from an authorized entity. If the attacker later wants to deny their involvement, they can claim that the command was legitimate and that they did not engage in any malicious activity. This creates a repudiation threat, as it becomes challenging to prove the authenticity of actions and transactions in the presence of sophisticated spoofing attacks.

Spoofing attacks entail the deliberate falsification of satellite signals or location information [28]. Attackers manipulate satellite signals, causing GSs or other satellites to track false positions or accept fraudulent data. Such deceptions can have severe consequences, including miscommunications, data manipulation, as well as compromised navigation and tracking systems [147], [20]. These spoofing attacks undermine the trustworthiness of satellite-derived information, posing significant risks to Satcoms operations [44], [24].

In addition to spoofing, Satcoms systems are susceptible to replay or forwarding attacks. These attacks intercept genuine satellite signals, which are then re-transmitted at a later time to deceive receiving stations [180], [67]. Attackers can effectively replay legitimate signals to create confusion or to manipulate communication exchanges. These actions introduce repudiation concerns, as attackers can deny their involvement in malicious activities, further complicating the attribution of such attacks [110].

3) Unauthorized Satellite Commanding: Unauthorized satellite commanding poses a significant threat to Satcoms systems, encompassing tampering and elevation of privilege threats [147], [28] within the STRIDE model [110]. Unauthorized satellite commanding occurs when an unauthorized entity gains access to the command and control systems of satellites, enabling them to issue commands without proper authorization. The consequences of such unauthorized access can be severe, ranging from disrupting a satellite's operation to altering its trajectory or rendering it inoperable [35].

Unauthorized satellite commanding constitutes a form of tampering with the satellite's control systems. Attackers, upon gaining unauthorized access, can manipulate critical functions, issue malicious commands, or tamper with satellite parameters. This tampering can lead to disruptions in communication, navigation, or surveillance services provided by the satellite [36].

Furthermore, unauthorized access to satellite control systems represents a significant risk in terms of the elevation of privilege [69]. Once inside the control systems, attackers may acquire higher levels of access and control than they originally had. This elevated privilege can enable them to not only issue disruptive commands but potentially compromise the entire satellite network, posing grave threats to the broader Satcoms infrastructure [44], [110].

The distinction between unauthorized satellite commanding and satellite hijacking (Section IV-B2) lies in their scope and impact. Unauthorized satellite commanding commonly refers to unauthorized access to some control system components of an individual satellite, potentially affecting its operations or functions. On the other hand, satellite hijacking often involves gaining unauthorized control over an entire satellite. We include unauthorized satellite commanding as a cyberattack vector for the overall Satcoms system to emphasize the importance of safeguarding individual satellites' control systems from unauthorized access, which, if exploited, could still have significant ramifications for the overall system. In essence, by including unauthorized satellite commanding as a cyberattack vector, we underscore the need for comprehensive cybersecurity measures that protect against a range of threats, from broader satellite hijacking to more specific and targeted attacks, such as unauthorized satellite commanding. A holistic approach to Satcoms security must address threats at both the level of individual components of a satellite as well as at the level of an entire satellite.

4) Satellite Constellation Vulnerabilities: Satellite constellations, composed of multiple interconnected satellites, are increasingly utilized to provide global and continuous coverage in modern Satcoms systems [28]. However, this interconnectedness introduces vulnerabilities that primarily fall into the STRIDE model classifications of tampering and DoS [44].

Attackers may exploit tampering vulnerabilities within satellite constellations [114]. This involves unauthorized access or manipulation of specific satellites within the constellation. For example, an attacker could target a particular satellite, compromising its communication links or control systems. Once control is established, this compromised satellite can serve as a launchpad for further attacks on other satellites in the constellation [16]. This tampering not only jeopardizes the compromised satellite but can have cascading effects, potentially compromising the operation of the entire constellation [114].

Another significant threat in the context of satellite constellations is the potential for DoS attacks. By targeting specific satellites, attackers can disrupt their communication links or control systems, rendering the satellites temporarily or permanently inoperable. Such attacks can lead to a significant degradation of the operation of the entire constellation, affecting a substantial portion of Satcoms services [188]. The interconnected nature of satellite constellations amplifies the impact of DoS attacks, making them a critical concern [114], [172].

5) Protocol Exploitation and Layer-specific Attacks: Satcoms systems rely on a diverse array of communication protocols that span various layers of the protocol stack for seamless data transmission and effective network control [49], [28]. These layers also introduce tampering, information disclosure, DoS, as well as elevation of privilege threats of the STRIDE model [110]. This section surveys attacks that manifest at different protocol stack layers, notably the physical, network, transport, and presentation layers [49].

a) Physical Layer Attacks [44]: At the lowest level of the protocol stack, the physical layer, attackers may target the RF signals that constitute the backbone of Satcoms [44]. These attacks can include signal jamming [44], spoofing [28], and eavesdropping [16], [67] as covered in Section IV-D.

b) Network Layer (Routing) Attacks: In the network layer, there is also the potential for routing attacks, which can disrupt the proper routing of data within the Satcoms network [189], [190], [191], [192]. These attacks can involve malicious routing updates, route diversion, or route poisoning, potentially leading to data misdirection or DoS scenarios [189].

c) Transport Layer Attacks: Advancing through the layers of the protocol stack to the transport layer introduces a range of pertinent attacks [193], [194]. Session hijacking, as an example, exploits vulnerabilities in transport layer protocols to illicitly access ongoing communication sessions [181]. This involves the interception of session identifiers or tokens, granting attackers control over legitimate communication channels [182]. Another area of concern is the manipulation of data packets during transmission, where attackers can modify packet contents, resulting in potential issues, such as data corruption or unauthorized access [105], [49].

d) Presentation Layer Attacks: Attacks that target the presentation layer of the protocol stack aim to exploit the formatting and encryption of data for malicious purposes [49]. By taking advantage of vulnerabilities in data compression or encryption mechanisms, attackers could potentially gain unauthorized access to sensitive information [49]. Furthermore, attackers may attempt to inject malicious code or malware into data streams, which could later compromise the integrity and security of the entire Satcoms system [24].

e) Authentication, Encryption, and Protocol-specific Vulnerabilities: Within each layer, the authentication and encryption mechanisms are pivotal for maintaining security [44], [49]. Compromising the authentication process [89], [90], [91], [92], [93] could enable unauthorized entities to gain access to the system, while exploiting weaknesses in encryption protocols [155], [195] may expose confidential data to interception and decryption [49].

Moreover, the unique security challenges posed by prominent Satcoms protocols, such as Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) [196], [197], [198], constitute another critical consideration [6], [53]. DVB-S2 plays a crucial role in satellite communications, offering enhanced data transmission capabilities. However, its adoption introduces its own complexities in terms of security considerations [53], [199], [200], [201]. DVB-S2 employs advanced modulation and error correction techniques to optimize satellite bandwidth, enabling higher data rates and improved transmission efficiency [202]. Yet, the increased complexity of data modulation also brings forth new challenges, including potential vulnerabilities that adversaries could exploit.

Understanding and addressing the DVB-S2 security nuances become paramount in ensuring the overall integrity and confidentiality of the communication channels [6], [53]. Research in the realm of DVB-S2 security is ongoing, and vigilance is required to stay ahead of potential threats. The interplay of authentication and encryption vulnerabilities, coupled with the protocol-specific intricacies of DVB-S2, underscores the need for a comprehensive security strategy within Satcoms systems [44], [49].

6) Cross-Segment Chain Attacks: Sophisticated attackers often exploit vulnerabilities that span multiple segments of the Satcoms system, introducing a range of threats such as tampering, DoS, and elevation of privilege in the STRIDE model [28], [24]. These cross-segment chain attacks highlight the interconnected nature of the Satcoms infrastructure and its susceptibility to multifaceted threats [114], [203].

Cross-segment chain attacks tamper with multiple segments of the Satcoms system. Attackers may initiate a cyberattack on the ground segment to gain unauthorized access to control systems. Subsequently, they can issue commands that compromise a satellite's onboard subsystems [44], [28]. By tampering with both the ground and space segments, attackers can undermine the integrity of the entire Satcoms system, jeopardizing its functionality and reliability [24].

The execution of cross-segment chain attacks can lead to DoS attack scenarios. By compromising communication links between ground and space segments, attackers can disrupt the flow of critical data and commands [44]. This disruption can result in mission failures, communication breakdowns, and potential safety risks, particularly if real-time communications are required for critical operations [20], [24]. Also, gaining unauthorized access to control systems in both the ground and space segments can provide attackers with elevated levels of control. These elevated levels of control can lead to malicious commands that compromise satellite operations, communication pathways, and the overall system integrity [24].

7) System-wide Supply Chain Attacks: The supply chain for Satcoms systems encompasses a network of entities, including satellite manufacturers, component suppliers, software vendors, and ground station contractors, all integral to the functioning of the Satcoms ecosystem [35]. System-wide supply chain attacks represent a critical threat vector capable of introducing various threat classifications of the STRIDE model [110] to the Satcoms infrastructure [12].

Attackers can exploit the supply chain's complexity and

TABLE IX: Types of cyberattackers on Satcoms systems.

Attacker Type	Subclassification	Motivation	Risk Level
State Entities	Nation-State	Political or Economic Gain	High
		Espionage [204]	High
		Cyberwarfare [205]	High
		Disruption of Services [6]	High
Non-state Entities	Hacktivists [143]	Social or Political Causes	Medium-High
		Online Activism	Medium-High
	Criminal Groups [21]	Financial Gain	High
		Data Theft and Ransom [94]	High
		Identity Theft	High
	Terrorists [206]	Propaganda and Disinformation	Medium-High
		Communication and Coordination	Medium-High
	Insider Threats [15]	Insider Attacks	High
		Unauthoriz. Access	High

interconnectedness to execute a range of attacks [152], [24]. Through spoofing, adversaries may mimic trusted entities, infiltrating counterfeit components and introducing fraudulent software, thereby compromising the integrity of Satcoms systems [36]. Tampering with the supply chain components opens the door to manipulation during production, transportation, or installation, enabling attackers to insert vulnerabilities, backdoors, or malware that compromise the entire Satcoms network [147]. The repudiation of involvement by attackers complicates attribution, making it challenging to trace the source of compromise and impeding effective incident response [110]. Additionally, information disclosure threats arise when adversaries gain unauthorized access to proprietary data, design specifications, and intellectual property, potentially leading to further cyberattacks or espionage [204]. Supply chain-based DoS attacks can disrupt operations, introduce delays, and even suspend critical Satcoms projects, with cascading impacts [24]. The compromise of supply chain entities can elevate attacker privileges, providing unauthorized access to sensitive systems and data, thereby granting control over the entire Satcoms network [28], [24].

F. Types of Attackers on Satcoms Systems

Cyberattacks against Satcoms systems can be carried out by a range of different parties or organizations, which can be roughly classified as either state or non-state entities [19]. The threat landscape for Satcoms is constantly evolving, and understanding the different types of attackers is crucial for effective defense strategies [206], [179]. Table IX summarizes the classification and characteristics of these entities.

1) State Entities: State entities [23] pose a significant threat in the context of Satcoms security. Nation-states may engage in cyberattacks for various reasons. One primary motivation is political or economic gain, whereby some nation-states may target communication channels to disrupt vital infrastructures or to steal sensitive information for strategic advantages [15]. Additionally, nation-states often conduct espionage by intercepting and monitoring Satcoms transmissions to gather intelligence about potential adversaries or to gain insights into military activities [23]. Cyberwarfare is another concern, where state-sponsored entities may target Satcoms to disable or manipulate critical satellite systems during times of conflict, causing disruptions or denying essential services to adversaries [151]. As a result, state-sponsored cyberattacks against Satcoms typically carry a high risk level, necessitating robust security measures and continuous monitoring [110].

2) Non-state Entities: Non-state entities [15] encompass a diverse array of attackers, each with unique motivations and capabilities. Hacktivists [143], driven by social or political causes, may target Satcoms to raise awareness about specific issues, promote their ideologies, or protest against certain policies [20]. Their attacks often involve the defacement of websites or DDoS attacks [207]. While hacktivist attacks might not pose a direct existential threat, they can cause significant disruptions and reputation damage [16]. Criminal groups [21], operating for financial gain, view Satcoms as lucrative targets for data theft, ransomware attacks [94], [208], and identity theft [69]. Such attacks can lead to substantial financial losses and compromise sensitive information. Terrorist groups may utilize Satcoms to propagate propaganda, coordinate activities, or communicate securely, making them a potential medium-high risk [206]. Furthermore, insider threats represent a significant concern in Satcoms security [105]. Employees or individuals with privileged access to Satcoms infrastructure may intentionally or inadvertently cause harm, leading to unauthorized access, data breaches, or system sabotage [23]. Managing insider risks requires a combination of technical controls, access restrictions, and personnel training [105].

G. Consequences of Cyberattacks on Satcoms Systems

In the literature, the possibility of all Satcoms failing simultaneously is classified as highly improbable, but not impossible [16]. The two major potential risks that can result in a complete Satcoms outage are a mega solar storm (known as the Carrington event [211]) or a space debris chain reaction (known as the Kessler syndrome [212]) and both are rare events [180]. In the same context, cyberattacks are frequently noted as an equally threatening and presently more realistic scenario [175]. Regardless of the probability, Van Camp and Peeters [180] demonstrated an effort to envision the significant harm that such a total Satcoms outage would cause for the world, whether as a result of a Carrington event, the Kessler syndrome, or a cyberattack. They exemplified our reliance on Satcoms data in numerous areas, such as GPS [173], weather forecasting [12], disaster management, air traffic control, and military communications [15], [94], [152], which may not be immediately apparent to the general public.

Generally, cyberattacks on Satcoms systems can have significant consequences and threats that could affect a range of industries and critical infrastructure. The main consequences, as summarized in Table X, include:

- Communication Disruption: Satcoms systems are widely used to provide communication services, especially in

TABLE X: Consequences of cyberattacks on Satcoms systems.

Consequences	Description
Communication Disruption	Deteriorated signal quality interrupts services. Emergency services, aviation, and military operations can be severely impacted [78], [152].
Data Breaches	Unauthorized access can lead to data theft, exposing sensitive user information, proprietary data, and operational plans [24].
Privacy Violations	Compromised user data can lead to identity theft, fraud, and loss of trust in service providers [209].
Misinformation and Manipulation	Attacks can lead to the dissemination of false information or manipulation of data, impacting decision-making processes.
Navigation System Manipulation	GPS jamming and spoofing attacks can mislead users, causing navigation errors, compromised safety, and disrupted operations [24].
Loss of Situational Awareness	Inaccurate or manipulated data can compromise situational awareness for users, from pilots to military personnel [210].
Physical Infrastructure Damage	Attacks targeting satellites and ground stations can result in hardware damage, rendering communication services unavailable.
Economic Impact	Industries relying on Satcoms can suffer financial losses due to disrupted operations, unavailability, and reputational harm [16], [6].
National Security Risks	Attacks targeting critical infrastructure and military communication systems can compromise national security [15].
Int. Relations, Geopolit. Tensions	State-sponsored attacks on Satcoms systems can strain international relations and escalate diplomatic tensions [151], [210].
Cyberwarfare and Espionage	State-sponsored attacks can compromise national security by gaining unauthorized access to military networks and classified information [23], [151].

areas where traditional terrestrial communication networks are not available [6]. Cyberattacks on Satcoms systems can disrupt communication services and result in a significant loss of communication capabilities [15]. This can have severe consequences for public safety, national security, and businesses that rely on Satcoms to operate [16]. For example, a DoS attack on a Satcoms system used by emergency services could lead to communication breakdowns and delayed response times, which could have a significant impact on saving lives [28].

- Data Breaches: Satcoms systems are used to transmit sensitive information, such as military intelligence, trade secrets, and financial data [17]. A cyberattack on Satcoms systems can result in the theft of such information, compromising the confidentiality and integrity of the data [36]. This can have significant economic and national security implications [99], [152].
- Privacy Violations: Attacks that compromise user data can result in privacy violations [209]. Personal and sensitive information can be exposed, leading to identity theft, fraud, and loss of trust in service providers [22], [209].
- Misinformation and Manipulation: Attacks on Satcoms systems can lead to the dissemination of false information or manipulation of data [209]. This can impact decision-making processes, from civilian navigation systems to military command centers [78], [152].
- Navigation System Manipulation: Satcoms systems rely on GPS for navigation and timing [28]. Cyberattacks on Satcoms systems can jam or spoof GPS signals, resulting in navigation errors [16], [143]. This can disrupt time-sensitive operations, such as financial transactions, transportation, and emergency services [28], [179].
- Loss of Situational Awareness: Inaccurate or manipulated data from Satcoms systems can lead to a loss of situational awareness for pilots, ship captains, and military personnel [210]. This can compromise safety and hinder effective decision-making [6], [20].
- Physical Damage: Satellites are valuable assets that can cost billions of dollars to manufacture and launch. Cyberattacks on Satcoms systems can cause physical damage to satellites, which can result in significant financial losses and impact space operations [12]. For example, a cyberattack that damages a satellite could cause a mission failure, resulting in a significant loss of investment [111].
- Economic Impact: Businesses and industries that rely on Satcoms can face significant financial losses stemming from disrupted operations, service unavailability, and reputational damage [12], [22]. Industries requiring tightly coordinated distributed assets, such as shipping, aviation, energy, and finance, are particularly susceptible to these disruptions [78], [49].
- National Security Risks: Attacks targeting critical infrastructure and military communication systems can compromise national security [15]. Unauthorized access to classified information, disruption of military operations, and compromised emergency response systems can have far-reaching consequences [152], [23].
- International Relations: State-sponsored attacks on Satcoms systems can strain international relations, leading to diplomatic tensions and escalations [151]. Attacks on communication systems can be considered acts of aggression in cyberspace [210].
- Cyberwarfare and Espionage: Satcoms systems are crucial components of military communications and intelli-

gence gathering [94]. Cyberattacks on Satcoms systems can be part of a larger cyberwarfare strategy aimed at disrupting military operations or stealing sensitive information [205], [151]. State-sponsored attacks or cyberwarfare can have severe geopolitical implications [204]. Attackers can gain unauthorized access to military communication networks, compromising strategic information, reconnaissance data, and classified communications [205], [151].

As outlined in Table X, these consequences and threats can have serious and far-reaching impacts, including substantial financial as well as control losses. The table also highlights the various mechanisms that attackers can use to cause these consequences.

H. Summary and Discussion

This section comprehensively surveyed the gamut of cyberattacks targeting Satcoms. The vulnerabilities of Satcoms systems were reviewed, following an organization scheme based on Satcoms segments and Satcoms-specific cyberattack categories. Section IV-B surveyed how the space segment can be compromised through hardware and software attacks as well as attacks that aim to hijack a satellite, to jam and interfere with satellite signals, or to inject and manipulate data. In Section IV-C, the forms of cyberattacks on the ground segment were comprehensively surveyed, including unauthorized access, data manipulation, exploitation of outdated or unpatched software, DoS, and network-based attacks. Additionally, Section IV-D detailed how Satcoms links can be targeted through the primary attack techniques used to obstruct data communications, such as link jamming and eavesdropping as well as signal spoofing and hijacking, citing recent cyberattack incidents [67]. Section IV-F identified the different entities that can target the Satcoms system, categorizing them as either state or non-state actors. Lastly, Section IV-G underscored the severe consequences of security threats to Satcoms systems and the probability of their exploitation, emphasizing the need for cybersecurity measures to protect these systems.

The main conclusion drawn in this section is that Satcoms systems are vulnerable to a wide range of cybersecurity threats, and no particular segment is immune. The growing frequency of cyberattacks against Satcoms providers suggests that these systems are being targeted by attackers for various purposes, with potentially significant consequences. Also, recent incidents have led to calls for strengthened cybersecurity measures among Satcoms network providers and emphasized the importance of proactive protection. Therefore, it is imperative that Satcoms providers prioritize their cybersecurity efforts and take a comprehensive approach to secure all aspects of their ground and space segments, as well as the Satcoms links (links segment).

V. Cybersecurity Strategies of Satcoms Systems

A. Overview and Organization

1) Overview of Satcoms Cybersecurity Strategies: A fundamental cybersecurity problem for Satcoms systems is that they have historically been designed based on the assumption that protection at their boundaries would be sufficient [111]. If the boundary was breached by an attacker, there was essentially no internal protection to contain the breach [6], [44]. However, Satcoms system designs should employ Defense in Depth (DiD) principles to slow down or severely restrict an adversary that has breached the outer boundary [12]. Whereby, both large traditional Satcoms deployments and modern rapidly developed New Space systems should have cyber-hardened designs that employ DiD principles throughout [19].

The DiD strategy should encompass multiple protection layers to safeguard the mission-critical assets in Satcoms systems [12]. More specifically, the DiD approach should holistically start with the acquisition, i.e., with secure supply chains and software development, include the hardening and monitoring of the Satcoms system, and extend to IDP, as well as the culture and people so that multiple layers of security control are formed [15], [69]. In particular, as per the segment structure in Figure 1, the security controls of the DiD strategy need to be employed in the space, ground, and links segments, so as to achieve a secure overall Satcoms system.

Furthermore, the introduction of automated satellite control systems into a historically human-operated space-mission environment brings new requirements for cybersecurity measures to ensure space system safety and security [172]. This is especially relevant on the ground segment side of satellite control, with the emergence of privately-owned communication antennas for rent and the general trend towards cloud-based operations and mission centers [216], [157].

2) Taxonomy Scheme of Satcoms Cybersecurity Strategies: This section comprehensively surveys the state-of-the-art of general Satcoms cybersecurity defense strategies and corresponding specific Satcoms cybersecurity techniques (mechanisms). We organize this survey of Satcoms cybersecurity strategies and techniques primarily according to the Satcoms segment, i.e., according to the space segment, the ground segment, and the links segment. In particular, the cybersecurity strategies and mechanisms for the space segment are covered in Section IV-B, see summary in Table XI, while the ground segment is covered in Section V-C (see Table XII), and the links segment is covered in Section V-D (see Table XIII). We distilled the categorization of the cybersecurity strategies and techniques from the comprehensive survey of the relevant Satcoms cybersecurity literature. We arranged the cybersecurity strategies and techniques following the general theme of progressing from securing an individual satellite payload or set of data to broader system-wide security strategies and techniques.

B. Space Segment Cybersecurity

In comparison to the RF communications realm, there has been very little research on the cybersecurity of the satellite payloads themselves [145]. This lack of research is most likely due to a combination of factors. First, historically, satellite payloads have been highly customized devices [6], [44]. Scholars seeking generally innovative scientific breakthroughs would find it difficult to extrapolate from problems relating to any one particular platform. This is made worse by the

TABLE XI: Space segment cybersecurity strategies and mechanisms.

Strategies	Mechanisms	Description and Specifications
Payload Security, Sec. V-B1	Payload Verif., Sec. V-B1a	Ensures payload integrity before and after deployment, and checks data accuracy [213].
	Payload Patching + Updating, Sec. V-B1b	Maintains cybersecurity through software/firmware updates [111].
	Anti-tamper, Sec. V-B1c	Prevents unauthorized access to satellite payloads [148].
Intrusion Detection and Prevention (IDP), Sec. V-B2	Onboard IDP Mechanisms	Real-time detection + prevention of cyberattacks on satel. payloads with signature-based analysis, anomaly detect., behavior-based analysis, and intrusion prevent. sys. (IPS) [214].
Remote Management and Control, Sec. V-B3	Remote Control and Monitoring	Manages payloads remotely using telemetry and command systems [215].

fact that satellite hardware is typically private and that access restrictions make such cybersecurity research difficult [112]. In addition, the space industry serves as a "gatekeeper" for many of these components and frequently expresses doubt or even antagonism toward security research [15].

Despite these obstacles, there has been some research on payload security [145], [112], [217]. According to Wheeler et al. [217], there are four broad attack surfaces: the onboard computer (which serves as the central integrating component for various subsystems and functions within the satellite), internal communications (such as SpaceWire buses), output systems (such as telemetry transmitters), and input systems (such as sensors and RF antennas). Wheeler et al. [217] also provide a top-ten list of payload vulnerabilities, which range from maliciously triggered safe modes caused by unhandled hardware states to sensor data buffer overflows caused by corrupted sensor data. Similarly, Falco et al. [112] recently detailed a process for constructing attack tree models in CubeSat platforms to discover the specific vulnerability and exploitation vectors. Through this process, they propose a number of scenarios involving platform compromise, such as a malicious payload delivered via compromised GSs. These attack models demonstrate how various exploit phases can be linked together to produce substantial negative cyber impacts.

Preventing such linkages through robust cybersecurity systems is the current standard protection against the majority of payload attacks [145]. Typically, Satcoms providers reduce the possibility that malicious parties will send control instructions to cause unexpected in-orbit behaviors by using the key strategies in Table XI. These strategies focus on ensuring the confidentiality, integrity, and availability of the satellite's data and its mission-critical payloads [217].

By implementing a range of cybersecurity strategies, Satcoms operators can establish a comprehensive DiD approach for the space segment [12]. This comprehensive DiD approach safeguards not only the sensitive data transmitted between satellites and GSs but also the overall integrity of the satellite's subsystems [106], [66]. It ensures that only authorized entities can access critical systems, while maintaining the continuous operation and availability of the Satcoms system, even in the presence of potential subsystem failures [24]. These strategies collectively bolster the resilience of space segment cybersecurity, thwarting potential payload attacks and contributing to the overall security of Satcoms networks [44]. As outlined in Table XI, the key principle to ensure a secure satellite payload is to employ one or more of the following cybersecurity strategies.

1) Payload Security: Satellite payloads are the heart of Satcoms systems, collecting and transmitting crucial data. Payload security mechanisms aim at ensuring the integrity, reliability, and confidentiality of this data. This section comprehensively covers the payload security mechanisms, which encompass payload verification mechanisms, payload patching, and updating, as well as anti-tamper mechanisms.

a) Payload Verification Mechanisms: Payload verification mechanisms are essential components of Satcoms cybersecurity, designed to ensure the integrity and reliability of satellite payloads both before and after deployment [213]. These mechanisms play a critical role in safeguarding against tampering and ensuring that the satellite's payload functions accurately, delivering precise and trustworthy data [218]. The following outlines the fundamental techniques and methodologies utilized for payload verification:

- Ground-based Testing [213]: One of the fundamental approaches involves testing the satellite's payload on Earth before it embarks on its journey into space. This ground-based testing phase is instrumental in verifying that the payload functions as intended. Engineers meticulously assess the payload's performance under simulated conditions, validating its ability to deliver accurate data.
- In-orbit testing [219]: In-orbit testing is a pivotal stage that occurs after the satellite has been launched and is operating in space. During this phase, engineers scrutinize the payload's performance in the actual space environment. This real-world assessment ensures that the payload functions optimally under the unique conditions of outer space, further enhancing its reliability.
- Data validation [220]: Data validation is an ongoing process crucial for confirming the accuracy of the information collected by the satellite's payload. This validation entails cross-referencing the satellite's data with data obtained from external sources, such as ground-based sensors or other satellites. By comparing datasets, engineers can identify any anomalies or discrepancies, ensuring the payload's data remains precise and reliable.
- Calibration [221]: Calibration periodically verifies and fine-tunes the satellite's payload. By calibrating the payload's instruments and sensors, engineers can guarantee that it continues to collect accurate and consistent data over time. This process is critical for maintaining the payload's reliability throughout its operational lifespan.

- Onboard diagnostics [222]: To monitor the health and performance of the payload components, onboard diagnostics tools are integrated into the satellite's payload. These tools continuously assess the functionality of various components, promptly detecting any irregularities or malfunctions. This proactive approach enables engineers to take corrective actions to ensure uninterrupted data collection.
- Remote sensing [215]: Remote sensing techniques are employed to validate the accuracy of the data collected by the satellite's payload. This validation often includes comparing the satellite's data with measurements acquired from ground-based sensors or data from other satellites. By cross-validating data from multiple sources, engineers can further ensure the integrity and reliability of the payload's information.

In addition to these techniques, recent advancements in satellite cybersecurity have introduced innovative approaches. For instance, a study by Hou et al. [223] introduced a framework that combines digital twin technology [224], [225], [226], [227] with verification techniques, specifically tailored for security monitoring and verification in satellites. This framework emphasizes the unique requirements of space missions and satellite systems. It offers methods for developing and synchronizing digital twins within such applications, enhancing the ability to monitor and verify security-related properties. Moreover, the framework introduces a verification engine capable of assessing properties in multiple temporal logic languages. Future work on this framework aims to develop a fully verified satellite digital twin system, which holds promising potential for enhancing payload verification in the Satcoms domain [223].

b) Payload Patching and Updating: Payload patching and updating are important aspects of maintaining the cybersecurity of satellite payloads [111]. Similar to other computer systems, satellite payloads are susceptible to security threats, necessitating regular updates and patches to address security vulnerabilities and enhance overall system performance [44], [158]. To fortify satellite payloads against potential cyberthreats, two key practices are employed:

- Payload Patching: This process applies updates and fixes to the software and firmware running on the satellite's payload [158]. It allows for the correction of security vulnerabilities and the enhancement of system reliability. Importantly, payload patching can be conducted remotely using specialized command systems, which enable operators to transmit software updates and patches to the satellite [44], [28], [228].
- Payload Updating: Payload updating replaces or upgrades hardware components within the satellite's payload [158]. These hardware components can encompass updating sensors, processors, and other critical systems to bolster their performance and capabilities, aligning them with evolving cybersecurity requirements [28]. Payload updating can also encompass software updates or modifications to the payload systems, especially if these updates are necessary to enhance the functionality, security, or performance of the payload.

Both payload patching and updating must be performed carefully and with strict adherence to security protocols [28]. Patches and updates must be tested thoroughly before they are deployed to the satellite, and proper backups must be taken in case of any issues during the patch or update process [229], [69]. By regularly patching and updating the hardware and software of the satellite's payload, the risk of security breaches can be reduced and the satellite's operational and effectiveness can be enhanced [44], [69].

Given the challenging nature of differentiating between cyberattacks and hardware malfunctions from ground-based observations, countering cyberattacks in the space segment is an intricate task [16]. The isolation of space amplifies this challenge, necessitating the development of robust forensic auditing capabilities before launch and their continued functionality even after a potential attack [111]. Establishing forensic auditing capabilities empowers space agencies and satellite operators to identify security breaches, assess their impact, and implement appropriate mitigation measures. These actions may include patching vulnerabilities, updating security protocols, and introducing additional security measures to prevent future attacks [158].

c) Anti-tamper Mechanisms: In the context of satellite cybersecurity, anti-tamper mechanisms serve as a critical line of defense against unauthorized access to a satellite's payload [148]. Anti-temper mechanisms encompass a range of techniques and technologies, including sensors, enclosures, and tamper-resistant coatings, which collectively fortify the satellite's resilience to physical and cyberthreats [229], [216].

- Sensors [148]: Sensors play a pivotal role in the detection of any unauthorized attempts to access the satellite's payload. These sensors are finely tuned to monitor various environmental and physical parameters. For instance, temperature sensors can discern alterations in temperature, potentially indicating tampering or unauthorized access to the payload. Similarly, pressure sensors detect changes in pressure, which could signify an intrusion attempt. The data generated by these sensors provides crucial insights into the security of the satellite's payload, enabling rapid response to potential threats.
- Enclosures [229]: Enclosures are designed with the primary objective of physically safeguarding the satellite's payload against unauthorized access. These protective enclosures often take the form of ruggedized cases or containers engineered to withstand the harsh conditions encountered in space. They are constructed with materials and designs that are resistant to tampering, making them exceedingly difficult to breach. Enclosures serve as an outer layer of defense, adding an additional barrier that must be overcome to access the payload. This DiD approach significantly raises the complexity and effort required for any malicious actor seeking access to the payload.
- Tamper-resistant Coatings [216]: Tamper-resistant coatings are applied to the surface of the satellite's payload to deter and detect tampering attempts. These coatings are specifically formulated to withstand physical manip-

ulation. If an unauthorized effort to tamper with the payload is made, these coatings might break, peel off, or otherwise show signs of disturbance, triggering an alarm or alert. Tamper-resistant coatings serve as a silent sentinel, silently monitoring the integrity of the payload's outer layers and swiftly notifying operators of any breach attempts.

Together, these anti-tamper mechanisms form a multi-layered defense strategy, creating a formidable barrier against unauthorized access to the satellite's payload [148]. This approach not only deters potential threats but also enables rapid response and mitigation in the event of an intrusion attempt. By combining sensors, enclosures, and tamper-resistant coatings, satellite operators can establish a robust cybersecurity framework that bolsters the security of the payload and contributes to the overall safeguarding of satellite-based communication systems [12].

In the context of enhancing satellite payload security and addressing the broader challenges of cybersecurity in various industries, the proposed Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, and Drone (SAAMD) technologies and communications, as introduced in [230], holds significant relevance. This cybersecurity testing lab offers a versatile and comprehensive platform designed to meet the cybersecurity needs of a wide range of industries.

The importance of this lab lies in its ability to serve as a valuable resource for evaluating and testing cybersecurity strategies across multiple domains, including satellite technology. It provides a controlled and adaptable environment for simulating various cyberattacks, including those targeted at satellite payloads and communication systems. As such, this testing lab plays a vital role in assessing the effectiveness of cybersecurity measures and strategies.

By offering a platform that can simulate real-world cyberthreats in satellite, aerospace, avionics, maritime, and drone technologies, the unified cybersecurity testing lab serves as a crucial tool for validating and refining the cybersecurity strategies discussed in this section. It allows researchers, industry professionals, and policymakers to evaluate the resilience of these strategies against a diverse range of cyberthreats, ultimately contributing to the development of robust and effective cybersecurity solutions for safeguarding critical infrastructure and technologies.

2) Onboard Intrusion Detection and Prevention (IDP): IDP systems are integral to satellite cybersecurity, dedicated to promptly identifying and thwarting security threats. In particular, onboard IDP systems, are pivotal for the real-time detection and prevention of cyberattacks aimed at a satellite's payload [214]. These advanced IDP systems function as a crucial line of defense, providing protection against a range of security threats, such as malware, viruses, and hacking attempts [231], [12], [232], [233].

Within the context of onboard IDP systems, Intrusion Detection Systems (IDSs) [82] stand as vigilant gatekeepers, continually monitoring the satellite's intricate systems and scrutinizing network traffic for any indicators of suspicious or unauthorized activities. IDSs employ a repertoire of techniques, including signature-based analysis, anomaly detection, and behavior-based analysis, allowing them to discern potential threats amidst the vast data streams [214]. When a potential threat is identified, the Intrusion Prevention Systems (IPSs) [160] spring into action, swiftly executing countermeasures to thwart the threat's attempt at compromising the satellite's payload. These countermeasures may include blocking malicious network traffic, isolation of affected systems, or even temporary deactivation of critical payload components to prevent further damage [214].

The significance of onboard IDP systems in defending the space segment cannot be overstated [12]. They serve as an essential safeguard, ensuring that the satellite's payload remains secure and operational, even when facing highly sophisticated security threats. Nevertheless, it is crucial to recognize that these IDP systems must be meticulously designed and rigorously tested to minimize false positives, as such inaccuracies can inadvertently disrupt the satellite's operations [214]. Moreover, they must possess the capability to operate autonomously, without the need for human intervention. This autonomy is essential due to the communication delays and other inherent limitations in the space environment, e.g., remoteness.

3) Remote Management and Control: Remote control and monitoring play a vital role in managing a satellite's payload, enabling administrators to oversee and operate the satellite's systems without requiring physical access [215]. This capability is particularly crucial in ensuring the cybersecurity of the satellite. Remote control and monitoring employ satellite telemetry techniques and command systems to manage the satellite's payload.

- Satellite Telemetry [94]: This process continuously collects data from various sensors and systems on the satellite. The collected data encompasses critical information, such as the satellite's position, orientation, velocity, and overall health status. Telemetry data is transmitted to GSs, where it is analyzed and serves as the foundation for monitoring the satellite's performance.
- Command systems [94]: Command systems empower operators to send precise commands to the satellite. These commands can range from orbit adjustments to the activation or deactivation of specific systems onboard the satellite. It is imperative to design command systems with robust security features to guarantee that only authorized personnel possess the capability to transmit commands to the satellite.

Typically, remote control and monitoring techniques are essential for managing the satellite's payload and ensuring its cybersecurity [111]. They empower operators to uphold the satellite's performance, to swiftly identify any anomalies or issues, and to respond promptly to security breaches and other potential threats [94], [215].

C. Ground Segment Cybersecurity

The ground segment of a Satcoms system refers to the network of ground-based infrastructures that communicates with the satellites to facilitate Satcoms [124]. The ground segment includes various components, such as GSs, SCCs,

TABLE XII: Ground segment cybersecurity strategies and mechanisms.

Strategies	Techniques/Mechanisms	Description and Specifications
Data Protection, Sec. V-C1	Encryption [155]	Safeguard data transmitted between GSs and satellites. Apply encryption algorithms, such as AES [87] and 3DES [234], to shield against interception and eavesdropping [155], [67].
Vulnerability Management, Sec. V-C2	Patch Management Process [69]	Maintain up-to-date systems and software. Employ a comprehensive patch management process to promptly apply security patches, mitigating potential vulnerabilities that could be exploited by attackers [16], [69].
Access Control/IDP Strategy, Sec. V-C3	Access Control, Sec. V-C3a	User Authentication [69], [235] and Authorization [89], Multi-Factor Authentic. [36], [236]: Ensure only authorized personnel can access the Satcoms system.
	Network Segmentation, Sec. V-C3b	Network Division [69]: Divide the ground segment, which encompasses multiple ground-based elements (such as GSs, MCCs, NOCs, SCCs, OMCs or user terminals), into distinct network segments to prevent system-wide compromises [237].
	Intrusion Detection + Prevention, Sec. V-C3c	Intrusion Detection Systems (IDSs) [12] and Intrusion Prevention Systems (IPSs) [15]: Monitor and detect suspicious activities using IDSs; identify threats and block or quarantine malicious network traffic with IPSs [238], [233], [239].

network operations centers, and other supporting equipment (see Sec. III-C). The ground segment is responsible for managing and controlling the communication between the satellite and the end-users, including managing the satellite's orbit, controlling its movements and functions, and monitoring its performance [84]. The ground segment also includes the systems responsible for processing and routing the data between the satellite and the users on the ground. Therefore, it is crucial to implement strong cybersecurity techniques on the ground segment to ensure the confidentiality, integrity, and availability of the Satcoms system [16]. This section comprehensively surveys the general strategies and specific techniques for securing the ground segment, see Table XII for an overview.

1) Data Protection: Data protection is a cornerstone of ground segment cybersecurity, safeguarding the confidentiality and integrity of information exchanged between the ground segment and the satellites [6]. In the context of safeguarding data within the ground segment of a Satcoms system, encryption ensures that data transmitted between the ground segment and the satellite remains secure and confidential [87], [234], [195]. The significance of encryption lies in its ability to restrict the access to and the decryption of transmitted data solely to authorized users [155]. Several encryption techniques are commonly employed in the ground segment [87], [186], [234], [240], each tailored to specific security and performance needs:

a) Advanced Encryption Standard (AES) [241], [89], [242]: The AES encryption algorithm is symmetric (i.e., the same key is used for encryption and decryption) and is widely used for safeguarding data within the Satcoms ground segment. Specifically, for ground segment security, the AES-Counter (CTR) mode [240] has emerged as a highly effective approach to simultaneously achieve robust security and optimal system performance. While the AES-CTR mode commonly utilizes key sizes of 128, 192, or 256 bits, the selection of a specific key size within this context should align with the required security standards. Overall, the well-established AES encryption method is widely applied in Satcoms systems to safeguard sensitive information, in the ground segment [69]. Ongoing research explores employing AES in layered encryption structures [243] and for image encryption on satellites [87], [244], [245].

b) Triple Data Encryption Standard (3DES) [234], [246]: 3DES is a symmetric encryption algorithm that uses three different keys to encrypt data [234]. Each data block is encrypted three times using the three keys, making it more secure than standard DES. However, 3DES is slower than AES, and its use is declining in favor of AES [246], [247].

c) Rivest-Shamir-Adleman (RSA) [41]: RSA, which is an asymmetric encryption algorithm, is extensively used for securing communications [69]. Utilizing a pair of keys, RSA employs a public key for data encryption and a private key for decryption. While RSA is commonly employed for various cryptographic purposes, with its primary application in digital signatures, it is also notably recognized for its role in securing sensitive information, including login credentials in Satcoms systems [41], [69], [248], [249].

d) Elliptic Curve Cryptography (ECC) [236]: ECC is an asymmetric encryption algorithm that generates keys with elliptic curves. ECC is generally more secure than RSA and uses smaller key sizes for the same level of security. This makes ECC faster and more efficient than RSA. Therefore, ECC is employed for lightweight access and data protection in Satcoms systems [250], [251], [252], [253].

e) Secure Hash Algorithm (SHA) [195]: SHA is a family of cryptographic hash functions that convert any input data into a fixed-length output [195]. The output, i.e., the hash, is a unique representation of the input data, making it impossible to reverse engineer the input from the hash. SHA is used to verify the integrity of data, as any change to the data will result in a different hash value. SHA is widely used for securing Satcoms [250], [254] and efficient SHA implementations based on Field Programmable Gate Arrays (FPGAs) have been developed for Satcoms systems [255], [256].

Generally, the use of encryption is a critical component of securing the ground segment of a Satcoms system; however, it is important to choose an appropriate encryption algorithm based on the specific required level of security and the performance demands of a Satcoms system [155].

2) Vulnerability and Patch Management: Vulnerability management is a critical process that involves the identification, assessment, and mitigation of vulnerabilities within a system or network. Complementary to this, patch management focuses on applying timely updates to software and systems to rectify known vulnerabilities [16], [69]. A patch is a targeted software update designed to address recognized system vulnerabilities [28]. Patch management involves the identification of vulnerabilities, their prioritization based on risk, rigorous testing, and the deployment to the system [118]:

1) Vulnerability scanning: Automated tools for systematic vulnerability scanning of the network infrastructure can efficiently identify known vulnerabilities [111].
2) Patch prioritization: After identifying vulnerabilities, a crucial step is the prioritization of patches based on risk levels [111]. This strategic prioritization addresses the most critical patches first, especially those susceptible to exploitation by potential attackers.
3) Testing patches: Rigorous testing is essential before deploying patches to the production system, ensuring their effectiveness and assessing potential side effects [28]. Conducting tests in a controlled test environment minimizes the risk of disrupting system functionality or introducing new issues [69].
4) Automated patch deployment: The automation of the patch deployment significantly enhances the efficiency and reduces the response times, particularly for large-scale or geographically dispersed networks [173], [213]. Automated tools are configured to deploy patches as soon as they become available, promptly securing systems against known vulnerabilities.
5) Change management process: The change management process, as a structured framework for managing system modifications [121], ensures methodical implementation with careful consideration of potential impacts. Documenting changes, obtaining stakeholder approvals, rigorous testing, and controlled deployment minimize disruptions and maintain system integrity [106].
6) Rollback plan: Despite thorough testing, patches can occasionally introduce unforeseen issues [111]. In such cases, a rollback plan is crucial. This plan comprises predefined procedures for reverting the system to its previous state, mitigating disruptions caused by problematic patches [28], and ensuring rapid system restoration for enhanced resilience [69].

The outlined patch management plays a pivotal role and is common practice for maintaining the security of the ground segment in Satcoms systems [118], [213], [28].

Additionally, regular data, software, and configuration backups are conducted in the ground segment [111], [69]. In the absence of a robust backup and recovery plan, Satcoms segments are at high risk of data loss or extended downtime during cyberattacks or hardware failures [15], [69]. Off-site backup locations can safeguard data from physical disasters, such as fires or floods [15]. A comprehensive disaster recovery plan, encompassing procedures for data and application restoration, identification of critical systems, and prioritization of recovery, is crucial [69]. Regular testing of the backup and recovery plan ensures its effectiveness and efficiency, facilitating the recovery of data, software, and configuration settings to their prior states [69], [67].

Lightman et al. [157] have recently developed a cybersecurity profile for the ground segment of satellite operations. This profile, integrated into a broader risk management plan, assists organizations in effectively managing cybersecurity risks associated with their Satcoms systems [69].

3) Access Control/IDP Strategy: The access control/IDP strategy for a Satcoms system comprises several key components aimed at safeguarding the ground segment's security:

a) Access Control: Access Control is the critical process of managing who has access to a Satcoms system and of defining the actions they can perform within the Satcoms system [257], [258]. Robust access control measures are essential for preventing unauthorized access to the communication system within the Satcoms ground segment [16]. Effective access control commonly encompasses user authentication and authorization [89], and Multi-Factor Authentication (MFA) [236]. MFA introduces multiple layers of security by mandating that users provide two or more forms of authentication before gaining access [171]. MFA typically combines traditional username and password authentication with more advanced techniques, e.g., biometrics and smart cards. MFA should be broadly examined for and adopted in Satcoms systems [236].

User authentication, i.e., verifying individuals' identities seeking access [171], and authorization, i.e., defining user actions and resource access [89], form the first lines of defense in securing the ground segment. In addition to traditional usernames and passwords, advanced biometric technologies, such as fingerprint or retina scans, can enhance user authentication for Satcoms systems [235]. Smart cards with cryptographic keys add a layer of security to the authentication process, e.g., in 5G systems [69], and should be explored for Satcoms systems. Also, Role-Based Access Control (RBAC), which establishes user roles and responsibilities by allocating access rights based on these predefined roles, e.g., in smart grid systems [259], should be adapted to the Satcoms context.

In addition to traditional authentication methods, Digital Signature Algorithms (DSA) and Elliptic Curve Digital Signature Algorithms (ECDSA) are employed for authentication purposes in Satcoms systems [260]. DSA and ECDSA utilize public and private key pairs to verify the authenticity of users and to ensure the integrity of transmitted data. These signature algorithms provide an additional layer of security, particularly when ensuring the origin and integrity of critical communications within the ground segment. The selection of key sizes for DSA and ECDSA is crucial and should align with the required security standards [253].

b) Network Segmentation: Network segmentation divides a network into smaller sub-networks to prevent an attacker from compromising the entire system [237]. The ground segment should be divided into multiple network segments to isolate different parts of the network. This can be achieved through the use of firewalls [261] and Virtual Local Area Networks (VLANs) [262].

Firewalls regulate and control traffic flows between different network segments [261]. Firewalls serve as barriers against unauthorized access attempts, actively monitor network traffic, and log events for subsequent analysis [261]. Firewalls can be strategically positioned at multiple locations within the network topology, including the network edge, between various network segments, or on individual hosts [69], [67]. This versatile deployment ensures a multi-layered defense mechanism that can help to effectively safeguard critical network boundaries [171].

VLANs are logical networks that group devices together based on their functionality, rather than their physical location [262]. VLANs can segregate different components within the network, such as the control network, data network, and management network [69]. This isolation is paramount for ensuring security as it prevents unauthorized access, limits the propagation of malware, and maintains the integrity of distinct network segments [262].

Incorporating network segmentation through firewalls and VLANs not only fortifies the overall security posture of Satcoms ground systems but also provides granular control over network traffic, enhancing the ability to detect and mitigate potential threats effectively.

c) Intrusion Detection and Prevention (IDP): In the context of Satcoms cybersecurity, IDP systems encompass a suite of techniques and tools designed to monitor and safeguard the ground segment against cyberattacks [82], [263], [231]. These IDP systems typically comprise both an IDS and an IPS, operating collaboratively to detect and thwart potential cyberthreats. It is imperative to conduct regular updates and maintenance for both the IDS and IPS components to uphold the security integrity of the overall IDP system [49].

The IDS focuses on threat detection with several general techniques that can be readily tailored for Satcoms systems cybersecurity [239], [266], [82], [263], [231]:

- Signature-based detection [267], [82] scans network traffic for specific patterns or signatures associated with known threats, effectively blocking recognized threats using a signature database.
- Anomaly-based detection [268], [269], [270], [271] identifies unusual or suspicious behavior within network traffic. Machine Learning (ML) algorithms (see Section V-D3) can establish a baseline of normal behavior, enabling the system to detect deviations and identify novel threats [49].
- Host-based intrusion detection [268], [231] monitors the activities of individual devices to detect signs of intrusion, specifically targeting attacks on single devices.
- Network-based intrusion detection [268], [272], [273] monitors network traffic to detect signs of intrusion, identifying attacks aimed at multiple devices on the network.

Complementing IDSs, IPSs assume a proactive role in cybersecurity [15], [24]. Going beyond access control firewalls [261], IPSs actively block or prevent attacks, such as blocking suspicious network traffic or quarantining infected devices [15].

Security Information and Event Management (SIEM) solutions collect, correlate, and analyze security event data from various sources in the network [274]. By providing real-time alerts and facilitating forensic analysis, SIEM systems enable the rapid detection and response to security threats, enhancing overall network security. [111].

D. Satcoms Links Cybersecurity

The uplinks and downlinks of Satcoms systems are integral for ensuring secure and reliable communication between GSs and satellites [16], [41]. Cybersecurity measures for the uplinks and downlinks are critical, as these points are primary targets for cyberattacks due to the transmission of information between satellites and GSs. To safeguard the links segment from cyberthreats, it is imperative to implement appropriate cybersecurity measures. Similar to the ground segment (see Section V-C), these measures include the application of data protection strategies, such as encryption mechanisms [155], access control through authentication [89], and the deployment of IDP mechanisms [214].

It is essential to note that vulnerability management, often associated with patch management (Sec. V-C2), may not be directly applicable to the links segment as vulnerability management often relies on addressing software-related vulnerabilities. However, the links segment predominantly involves dedicated hardware components rather than software systems. In addition to encryption, authentication, and IDP mechanisms, as outlined in Table XIII, frequency-hopping [186] and spread spectrum mechanisms [41] are commonly employed to enhance the security of the uplinks and downlinks.

1) Frequency-Hopping: Frequency-hopping is a widely adopted technique in Satcoms systems to enhance the security and reliability of communication links [41]. This technique involves rapidly switching the carrier frequency of the transmitted signal over a wide frequency range [49]:

- Pseudo-random Sequence Generation: At the core of frequency-hopping lies a pseudo-random sequence generator [186], which produces a sequence of frequencies that the transmitter will traverse during communication. The critical aspect is the unpredictability and apparent randomness of this sequence, rendering it inscrutable to potential attackers.
- Frequency Synthesis: A frequency synthesizer generates the frequency signal that the transmitter employs [13]. The frequency synthesizer adheres to the frequency sequence generated by the pseudo-random sequence generator, ensuring precise synchronization [186].
- Synchronization Mechanisms: Achieving synchronization between the transmitter and receiver is paramount to the effectiveness of frequency-hopping [264]. A synchronization signal is concomitantly transmitted with the data, serving as a reference for the receiver. The receiver leverages this signal to synchronize seamlessly with the frequency-hopping sequence, ensuring uninterrupted communication [264].

TABLE XIII: Satcoms links cybersecurity mechanisms and specifications

Mechanism	Specification	Description
Frequency-Hopping, Sec. V-D1	Pseudo-random Sequence Generation [186]	A pseudo-random sequence generator produces a sequence of frequencies for the transmitter to traverse during communication. The unpredictability and randomness of this sequence make it inscrutable to potential attackers.
	Frequency Synthesis [13]	A frequency synthesizer generates the frequency signal, adhering to the pseudo-random sequence, ensuring precise synchronization between transmitter and receiver.
	Synchronization Mechanisms [264]	A synchronization signal is transmitted with the data to allow the receiver to synchronize with the frequency-hopping sequence, ensuring uninterrupted communication.
	Narrow-Band Filtering [85]	Narrow-band filtering at the receiver matches the current frequency of the incoming signal, allowing only the desired signal to be received while filtering out extraneous noise.
	Use in Conjunction with Encryption [186]	Frequency-hopping can be used alongside encryption to enhance communication link security.
Spread Spectrum, Sec. V-D2	Direct-Sequence Spread Spectrum (DSSS) [49], [41]	DSSS broadens the signal's bandwidth by multiplying it with a high-frequency code, enhancing security and resilience to interference.
	Frequency-Hopping Spread Spectrum (FHSS) [186], [41]	FHSS rapidly switches between different frequencies in a predefined sequence, making it challenging for attackers to intercept or disrupt the signal. Effective in interference-prone environments.
	Orthogonal Frequency Division Multiplexing (OFDM) [265]	OFDM divides the signal into orthogonal sub-carriers, increasing data rates and resistance to interference.

- Narrow-Band Filtering: To further enhance the signal fidelity and protect against unwanted signals and interference, narrow-band filtering is employed at the receiver end [85]. This filtering mechanism is finely tuned to match the current frequency of the incoming signal, ensuring that only the desired signal is received while filtering out extraneous noise [85].

Frequency-hopping, with its various mechanisms, can be effectively combined with other security measures such as encryption [186]. For instance, [279] proposed a novel approach to improve the cybersecurity of a LEO satellite link by utilizing less vulnerable frequency bands and highly directional antenna beams. The approach enhanced security by communicating within a specific angle of arrival, minimizing transmitter power, and optimizing gain patterns for improved signal-to-noise ratio.

2) Spread Spectrum: Another crucial technique in Satcoms links is spread spectrum, which spreads the signal over a wide frequency band, increasing security and reliability [49], [41]. This technique is achieved through modulation with a spreading code, expanding the signal bandwidth and making it challenging for attackers to intercept or jam the signal. Three primary spread spectrum techniques are used in Satcoms links:

- Direct-sequence Spread Spectrum (DSSS): DSSS spreads the signal by multiplying the data signal with a high-frequency code, thereby broadening the signal's bandwidth. Subsequently, the receiver employs the same code to despread the signal back to its original bandwidth [49], [41]. This technique enhances the signal's resilience to interference and augments security.
- Frequency-hopping Spread Spectrum (FHSS): FHSS spreads the signal by rapidly transitioning between different frequencies in a predefined sequence. This continuous frequency hopping makes it exceedingly challenging for adversaries to intercept or disrupt the signal. The receiver synchronizes with the hopping sequence to reconstruct the original signal. FHSS is particularly effective in environments prone to significant interference, as it enables the signal to avoid problematic frequencies [186], [41].
- Orthogonal Frequency Division Multiplexing (OFDM): OFDM divides the signal into multiple sub-carriers that are orthogonal to each other, meaning they do not interfere with one another. The signal is then distributed across these sub-carriers, substantially increasing data rates and bolstering resistance to interference [265].

Each of these spread spectrum techniques has its advantages, and the choice depends on the specific requirements of the Satcoms system [185]. Combining spread spectrum mechanisms with Multiple Input Multiple Output (MIMO) antenna structures further enhances security [280], [281].

It is crucial to recognize that the security of the links segment relies on a layered security approach that incorporates multiple techniques to ensure robust protection [49]. Regular security audits, updates, and patches are fundamental for maintaining the security of the links segment [111], [69].

3) Machine Learning for Satcoms Links Cybersecurity: As detailed in Table XIV, a subset of studies has focused on adapting ML approaches to the specific context of Satcoms links cybersecurity. These ML-based IDSs utilize supervised and unsupervised ML algorithms, Deep Learning (DL) models, distributed IDS models, and Federated Learning (FL) to detect and classify cyberthreats in Satcoms networks.

While these ML-based IDS functionalities can be deployed as microservices at either end of a link connection (ground or satellite), their primary role is to inspect traffic traversing the links segment, acting as a protective filter against potential

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2024.3408277

TABLE XIV: Machine Learning (ML) for Satcoms links cybersecurity, Section V-D3

Mechanism	Specification	Description
ML-Based IDSs	Supervised and Unsupervised ML Algorithms [95], [207], [266]	ML is used to develop IDSs for detecting and classifying cyberattacks in Satcoms networks, including DoS, DDoS, and zero-day attacks. Supervised and unsupervised ML algorithms may be employed for better classification.
Deep Learning (DL)-Based IDSs	DL Models [238], [239], [266]	Deep Learning models, such as LSTM-RNN and GRU, are utilized for robust IDSs in Satcoms capable of dealing with unlabeled data and detecting zero-day attacks.
Distributed IDSs Models	IDSs Models for Distributed Satcoms Networks [239], [272], [275]	IDSs models are proposed for distributed networks, improving security across domains and efficiently allocating resources for malicious traffic analysis and elimination.
Federated Learning (FL)-Based IDSs	FL for Distributed Satcoms IDSs [239], [272], [276], [277], [278]	FL is employed for distributed IDSs to enhance malicious traffic recognition, packet loss, and CPU utilization. Models, e.g., CNNs and GRUs may be used for threat identification.

attacks. We acknowledge that different Satcoms systems may have different specific communication protocols and data types and further research should explore the adaptability of the various proposed IDS mechanisms to these specific protocols and data types.

One specific research direction is the detection and classification of attacks in Satcoms networks [238], [282] with DoS, DDoS, and zero-day attacks as common attacks, which can cause disruptions or decrease the service quality [207], [239]. Several studies have leveraged ML techniques to design IDSs capable of discerning between normal traffic and malicious activity [95], [283], [207]. For instance, Yap et al. [282] developed IDSs utilizing a decision-tree ML algorithm to detect cyberattacks across various threat vectors, including DDoS. However, it is noteworthy that the study employed only one supervised ML algorithm for training and classifying different cyberattack types. To ensure the suitability of the ML algorithm for specific Satcoms settings, future research should compare multiple supervised ML algorithms. This comparative analysis would provide insights into identifying the most effective classifier for Satcoms security. Additionally, exploring unsupervised learning approaches in future research can contribute to a more comprehensive understanding of ML-based IDSs in the context of Satcoms networks.

Since accessing large sets of labeled data from the Satcoms network is difficult, many conventional ML algorithms are incapable of achieving high accuracy [238]. Zhu et al. [238] used a DL model to present a robust IDS model for dealing with unlabeled data. While claiming better performance and elasticity, this model only examined the main security issues in an unlabeled context and lacks statistical verification of model robustness across a variety of contexts involving mixed labeled and unlabeled data. In a related effort, Koroniotis et al. [207] developed an IDS-based framework rooted in DL. This framework utilized a Long Short-term Memory Recurrent Neural Network (LSTM-RNN) and a Gated Recurrent Unit (GRU) approach. Comparative analysis against five supervised and two unsupervised ML algorithms demonstrated the superiority of their LSTM-RNN and GRU-based IDS approach over existing rule-based IDS tools, particularly in detecting zero-day attacks. While the evaluation results affirm the model's efficiency, it is essential to note that the model is constrained to a centralized version of DL. Additionally, the scalability of the framework for handling heterogeneous data sources, characteristic of Satcoms networks, poses an open challenge for future research.

Wen-bo et al. [275] introduced a security domain incorporating a login and log-out mechanism, along with a satellite network distributed IDS model. They also developed a cooperative IDS mechanism that operates both within and between security domains. Simulation results affirm the suitability of the IDS model and cooperation mechanism for satellite networks. Li et al. [272], on the other hand, proposed distributed IDSs utilizing FL to efficiently allocate resources in each domain for the analysis and elimination of malicious traffic. Their model demonstrated superior performance compared to traditional DL and IDSs, particularly in terms of malicious traffic recognition, packet loss reduction, and CPU utilization.

Also, Li et al. [276] introduced DeepFed, an FL-based IDS framework designed for cyber-physical systems. To establish relevance for Satcoms, it is noteworthy that cyber-physical systems share certain characteristics with Satcoms networks [239], and DeepFed exhibits promise for adaptation to Satcoms systems, warranting examination in future research. For threat identification, DeepFed utilizes a combination of Convolutional Neural Networks (CNNs) and GRUs. In a related study, Chen et al. [277] proposed FedAGRU, an FL-based attention GRU, to identify attacks and eliminate minimal contributing updates, resulting in a highly effective global model with minimal communication costs. While [278] presents an FL-based approach for wireless IDSs, it should be investigated for its applicability to Satcoms links in future research. Evaluation results indicate the effectiveness of these models; however, concerns persist regarding their ability to scale up to handle heterogeneous data sources found in Satcoms networks. Additionally, addressing the requirements for traffic security and privacy in the Satcoms context necessitates further data pre-processing to enhance privacy guarantees. Salim et al. [239] proposed an extensive Deep FL, a centered model for preemptively detecting intrusions in Satcoms networks by leveraging decentralized on-device data while upholding data privacy However, further validation and refinement of the model are required using real-world Satcoms datasets. Additionally, there is a need for efforts to establish optimally harmonized parameters to enhance accuracy.

Furthermore, the expansion of networks of LEO satellites, coupled with the evolution of communication systems towards B5G and 6G, may create opportunities for cyberattacks that pose severe risks to the Satcoms infrastructure. To address this issue, a random routing algorithm is proposed in [189] to prevent DDoS attacks on LEO satellite constellation networks. This algorithm utilizes classical algorithms with randomness and a weighted probability distribution to increase uncertainty and improve network functionality. In the same context, [284] proposed a physical layer solution that uses the inherent physical properties of the channel to ensure cybersecurity against man-in-the-middle attacks launched from aerial platforms. This solution extracts noisy variations from the received signal using wavelet filtering and processes it through a deep neural network based on LSTM to identify legitimate satellites and spoofing APs with an accuracy of over 98%.

E. Summary and Discussion

This section comprehensively surveyed the state-of-the-art of general cybersecurity strategies and specific cybersecurity mechanisms (techniques) employed by Satcoms systems. Satcoms systems were historically designed with protection at their boundaries only and lacked internal protection. Therefore, there is now a need to implement a DiD strategy with multiple layers of security controls, including acquisition, secure supply chains, space system hardening and monitoring, secure software development, IDP, as well as culture and people, so as to secure mission-critical assets. We have comprehensively surveyed these cybersecurity measures required for Satcoms systems, covering the space segment, the ground segment, and the links segment.

For the space segment, several cybersecurity mechanisms can ensure secure satellite payloads, including payload verification, anti-tamper mechanisms, and onboard IDP, see Section V-B. The ground segment, which manages and controls communication between the satellite and the end-users, requires several cybersecurity mechanisms, including encryption, access control, and network segmentation, see Section V-C.

The uplink and downlink are prime targets of cyberattacks, necessitating appropriate cybersecurity measures to protect these links. The state-of-the-art link protection techniques encompass frequency-hopping and spread spectrum mechanisms, as comprehensively surveyed in Section V-D. Importantly, the security of the links segment is only as strong as the weakest link. Therefore, it is essential to implement a layered security approach that incorporates multiple techniques to ensure the security of each link of the links segment.

VI. Learned Lessons

Drawing insights from the thorough examination of Satcoms cyberattacks and cybersecurity strategies presented in the previous sections, we synthesize the following main learned lessons for designing and operating modern Satcoms systems that strive for the cybersecurity goals in Section II-C. The learned lessons section focuses on the implications of the preceding Sections IV and V that—in our view—are of immediate relevance and applicability for Satcoms cybersecurity. Longer range issues that—in our view—are of relevance for future years are outlined in Section VII.

We organize this learned lessons section following a sequential ordering scheme that progresses from the prevention of attacks (Section VI-A), to the defense against active attacks (Section VI-B), and to the recovery after attacks (Section VI-C). Additionally, learned lessons relating to the integration with 5G/6G systems are presented in Section VI-D.

A. Attack Prevention

Within the domain of Satcoms cybersecurity, proactively mitigating risks through attack prevention [26] is very important [285]. To fortify the defenses against potential threats targeting Satcoms systems, a comprehensive array of preventative strategies is imperative [37], [111].

1) Compliance with Regulations and Standards: Satcoms are subject to stringent regulations and standards to ensure their secure and reliable operation [16], [15], [6]. One of the key frameworks guiding this compliance is the National Institute of Standards and Technology (NIST) Cybersecurity Framework [12]. Adhering to these established regulations and standards provides a structured approach to addressing potential vulnerabilities and mitigating risks associated with cyberthreats [209] so as to safeguard the integrity of Satcoms systems and to protect sensitive information [69]. Specifically, compliance helps with:

- Security Assurance: By aligning with established frameworks, such as the NIST Cybersecurity Framework [12], Satcoms operators can gain confidence that their systems are fortified against cyberattacks and data breaches [12].
- Data Protection: Sensitive data transmitted through Satcoms, including military communications, financial transactions, and critical infrastructure control, must be shielded from unauthorized access. Regulatory compliance helps ensure the confidentiality, integrity, and availability of this data [209].
- Operational Reliability: Compliance measures contribute to the overall reliability and resilience of Satcoms systems. This is especially crucial in scenarios where communication breakdowns could have threatening consequences [69].
- Legal and Regulatory Adherence: Non-compliance with industry regulations can result in legal penalties, loss of licenses, and damage to an organization's reputation [12], [15], [27].

The design of Satcoms systems necessitates a substantial and varied range of engineering disciplines. The emerging industry for small satellites is putting additional pressure on the system design schedules and security [115]. Therefore, cybersecurity cannot be ignored. Standard cybersecurity engineering practices will be crucial. Their necessity will continue

This article has been accepted for publication in IEEE Communications Surveys & Tutorials. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/COMST.2024.3408277

to evolve in the ground, space, and links segments since the designers may traditionally only be concerned with protecting against benign faults and threats from the hostile physical orbital environment [16].

2) Continuous Monitoring and Threat Intelligence: In the ever-evolving landscape of cybersecurity, the vigilance provided by continuous monitoring and the insights from threat intelligence are indispensable [274], [69]. These proactive measures enable the timely detection and response to cyberthreats in real-time [111]:

- Secure Authentication and Authorization Mechanisms: Satcoms systems should use secure authentication and authorization mechanisms to ensure that authentication credentials are properly managed and protected [69]. This could include strong passwords, multi-factor authentication [236], and role-based access control [259].
- SIEM Systems: SIEM systems holistically collect and meticulously analyze security data originating from both internal systems and external sources [111], [274].
- Harnessing Threat Intelligence: To stay ahead of adversaries, it is imperative to tap into threat intelligence feeds. These sources provide invaluable, up-to-the-minute information on the latest threats and vulnerabilities [69], [110]. Armed with this knowledge, organizations can proactively fortify their defenses [110].
- Regular Security Assessments and Testing: Regular security assessments and penetration testing can systematically identify vulnerabilities and assess the effectiveness of existing security controls [69]. Furthermore, they facilitate the fine-tuning of security strategies [44].
- Threat Modeling for Strategic Prioritization: A well-informed approach to security should include threat modeling exercises [69]. These exercises illuminate potential threats and vulnerabilities within the system, enabling prioritization based on their potential impact [110].
- Validation and Auditing: Continuous vigilance requires regular system testing and validation [69]. This ensures that the system remains secure and operates as expected. Complementing this, periodic security audits serve as critical checkpoints for assessing adherence to security protocols [111].
- Intrusion Detection and Resilience Systems: Intrusion detection and resilience systems can be used to detect and respond to security incidents in real-time [214]. This includes the use of anomaly detection systems, log monitoring, and incident response plans [69].

3) Attack Resilience Planning: In the ever-evolving landscape of Satcoms systems security, attack resilience planning has emerged as an indispensable cornerstone [285], [37]. This strategic framework comprises three pivotal components, each designed to safeguard the integrity, reliability, and functionality of Satcoms systems even when confronted with cyberthreats [26], [149].

a) Identifying a Minimal Subset: At the core of this planning is the identification of a minimal subset of satellite components. This carefully curated set represents the mission-critical essentials required for the satellite to perform steadfastly under all circumstances, including uninterrupted communication with GSs [26]. By isolating these critical elements, a foundation is laid for unwavering mission continuity.

b) Reducing the Attack Surface: Minimizing the attack surface is a paramount objective in safeguarding satellite systems. Only authorized GSs should have the capability to communicate with the satellite, employing secure and encrypted communication channels. The adoption of the Communications Security (ComSec) protocol [111] is a crucial step in securing wireless links and ensuring that satellite commands are exclusive to authorized GSs. However, recognizing the potential limitations of this approach, it is imperative to implement additional security measures, such as access controls [286], [148], [287], firewalls [261], and IDSs [283], [207], so as to collectively restrict the avenues through which unauthorized entities could compromise satellite control.

Additionally, network segmentation and isolation strategies play a pivotal role in reducing the attack surface and enhancing security [237], [69]. This approach separates critical systems from less important ones, effectively containing the spread of an attack in case of a breach. Network segmentation can be achieved through:

- Firewalls [261]: Firewalls establish controlled boundaries between network segments and regulate traffic flows.
- VLANs [262]: VLANs logically segment the network and isolate different categories of devices and traffic.
- Air-gapping [237]: Air-gapping in Satcoms refers to a security measure that physically isolates critical systems, such as GSs or SCCs, from external networks, creating an additional layer of security. This physical isolation keeps the Satcoms systems physically disconnected from other networks, including the internet, to prevent unauthorized access and to reduce the risk of cyberattacks.

Integrating these measures into secure network design and reducing the attack surface improves the protection of Satcoms systems against unauthorized access and data breaches, bolstering their overall security posture [111], [69].

c) Implementing a Multi-Layered Security Approach: This approach implements multiple layers of security controls, encompassing both physical and logical measures [288], [69]. Physical security measures may include tamper-resistant hardware [216] and secure facilities. Logical security measures encompass access controls, IDP, and network segmentation [237], [69].

d) Contingency Planning: Satellite systems must be designed with contingencies, such as system failures, natural disasters, and cyberattacks, in mind [15]. Robust contingency plans are a linchpin in ensuring swift and efficient system recovery in the event of an incident [37], [217]. These plans must undergo regular review, updates, and rigorous testing to guarantee their effectiveness and adaptability to evolving threats and circumstances [28].

4) Regular Security Awareness Training: In order to maintain a robust security posture for Satcoms systems, it is imperative to institute continuous security training and awareness programs [69], [289], [24], [290]. These programs are essential to equip all individuals involved in the design, operation, and upkeep of the system with the necessary knowledge and skills to safeguard against security risks and adhere to best practices [111], [89], [69].

- Secure Coding Practices [69]: In-depth training on writing secure code to fortify the system against vulnerabilities and exploits. Secure coding practices should be followed during the development of satellite software to prevent vulnerabilities, such as buffer overflows, injection attacks, and race conditions [173]. This is especially important for critical components, such as C2 software [291], that could be targeted by attackers. Secure coding practices include using static code analysis tools, following secure coding guidelines, such as CERT C or MISRA C [292], and performing code reviews.
- Secure Network Design [261]: Instruction on creating and maintaining a secure network infrastructure to prevent unauthorized access and data breaches is crucial in Satcoms systems.
- Incident Response Procedures [292]: Guidance on how to swiftly and effectively respond to security incidents, minimizing potential damage.

5) Ensuring Third-Party Stakeholder Commitment to Security: In the context of Satcoms, collaborating with third-party stakeholders demands a rigorous commitment to security [69]. To gain access to the system, stakeholders must undergo comprehensive security assessments and adhere to established security guidelines [67]. Moreover, it is imperative to establish clear and detailed contractual agreements with third-party stakeholders, explicitly outlining their security obligations and accountabilities [69].

These agreements should provide a comprehensive overview of the specific security measures that third-party stakeholders must implement [24]. They should also outline the consequences of a security breach or non-compliance. Robust procedures for monitoring and auditing third-party stakeholders should be put in place to ensure ongoing compliance with security requirements [152].

B. Enhancing Defense Against Active Attacks

In the context of Satcoms security, defending against active attacks demands a multifaceted strategy [24]. This section covers the two key aspects of this defense: Defense in Depth (DiD) and the concept of Gradual Failure Mitigation.

1) Defense in Depth (DiD) Strategy: In Satcoms systems, a sophisticated approach to security can be adopted to address complex security challenges without the need to disable critical security measures [24]. Specifically, within the Satcoms context, it is essential to distinguish between layers of security. The outermost and most complex security layer, while highly effective, can be dynamically adjusted or “discarded” for operational purposes when authorized by a ground controller using the appropriate code. It is important to note that this outermost security layer—while being a significant component of the system's overall security strategy—may not encompass the core critical security measures. The core security measures would typically remain intact, ensuring the fundamental security of the system. The approach of dynamically adjusting or “discarding” certain security aspects aligns with the overarching principle of DiD [293]. This approach represents an adaptive and flexible way to manage security without compromising mission-critical functions.

DiD is a comprehensive security strategy that involves layering multiple security controls to create a resilient security posture [12]. In the context of satellite systems, it is particularly advantageous, as it allows for the implementation of multiple layers of security controls, thereby fortifying the system against a wide array of cyberthreats [157].

2) Gradual Failure Mitigation: Certain satellite commands inherently pose significant risks. To address this, Satcoms system designers should prioritize minimizing the occurrence of damaging commands and, in cases where they are unavoidable, the system designers should extend the time interval between issuing the command and reaching the point of irreparable damage [36]. This extended timeframe provides cybersecurity systems with a longer window for detecting and responding to compromises at the GS.

To further mitigate these risks, designers should incorporate gradual failure techniques, including fail-safes [111] and redundancy mechanisms [113]. These measures should be designed to minimize the impact of a wide range of failure events on the satellite system [69]. By embracing a combination of proactive command management and robust failure mitigation strategies, satellite systems can enhance their resistance to active attacks and bolster their overall security posture [111]. Whereby, proactive command management refers to the practice of taking preemptive measures to reduce the likelihood of potentially harmful or risky commands being issued to a satellite. In the context of Satcoms systems, it refers to a set of cybersecurity strategies aimed at minimizing the risks associated with certain satellite commands.

C. Recovery from Attack

In the challenging domain of Satcoms cybersecurity, recovery from potential attacks is very important for ensuring the continuity and reliability of these mission-critical communication systems. This section covers the self-recovery strategies that empower Satcoms to recover from adverse situations and cyberattacks. Unlike conventional ground-based systems, the processing capabilities of the Satcoms space segment, i.e., the spacecraft themselves, differ significantly in several aspects. One critical distinction lies in the solitude of the spacecraft and the requirement to operate autonomously without direct human contact for the duration of its mission, often spanning several years [24]. Given this inherent isolation, self-recovery mechanisms are very important [26].

In terrestrial systems, the ultimate source of trust and recovery lies in a human with access and maintenance tools. When a computer encounters an issue, human intervention is possible through corrective actions, such as unplugging, swapping components, or reimaging [69]. However, such a level of human intervention is often impractical for satellites operating in space. Consequently, satellites must be engineered to be self-reliant, and equipped with the capability to autonomously recover from failures. This autonomy can be achieved through self-recovery strategies, such as fault-tolerant design [16], self-checking mechanisms [294], [295], and autonomous recovery algorithms [296], [297]. These measures ensure that satellites can adapt and recuperate even in the challenging conditions of space environments and withstand the pressures of potential cyberattacks [26].

Some of the systems on the satellite may need to be restarted or rebooted in order to recover from an anomalous situation. Also, the satellite is putting its mission objectives on hold while it recovers [16]. Even if recovery ultimately succeeds, if the restart process for the satellite is excessively drawn out, just trying to recover may endanger a mission or cause it to fail. Moreover, there are instances in a satellite's life when recovery must be handled with extreme caution and executed slowly. For instance, when a satellite first enters orbit, it often undergoes a lengthy check-out period. During this phase, systems are thoroughly tested, and baseline performance is established [111]. This cautious and gradual approach to recovery ensures that the satellite's systems are functioning correctly and that any potential issues are addressed before the mission proceeds.

However, once in regular operation, the satellite systems should restart and operate as quickly as possible, ideally in a matter of seconds [111]. Cybersecurity systems should distinguish between a fault that necessitates a thorough system check on reboot and a commanded or autonomous reboot that may not. In case of further anomalies, different self-check subsets should be reactivated as needed.

D. Integration with 5G/6G Systems

In the integration of Satcoms with 5G/6G systems [47], [50], [298], [51], several crucial design considerations emerge to ensure both the security and efficiency of these integrated networks [69], [299]. First and foremost, designers must address the unique challenges and opportunities posed by 5G/6G technologies, including the possibilities for network slicing to isolate Satcoms traffic within the high-speed terrestrial 5G/6G networks [69], [300]. Moreover, optimizing cybersecurity mechanisms to operate seamlessly within the tight latency constraints of 5G/6G is paramount [301], [302], [14], [303].

Ensuring the security of satellite-to-GS communications [304] involves implementing robust encryption protocols [155], [195], strong authentication methods [236], and secure key management systems [49]. To bolster resilience, continuous monitoring with threat intelligence specific to 5G/6G is essential, complemented by SIEM systems capable of monitoring both Satcoms and 5G/6G networks [274], [69].

Additionally, network segmentation [237] should be applied to both satellite systems and 5G/6G infrastructures, with considerations for air-gapping critical components of satellite systems from 5G/6G networks in the event of a breach [69]. Secure coding practices should extend to 5G/6G components interfacing with Satcoms, accompanied by regular code reviews for critical functions [69]. Resilience systems should be designed to adaptively detect and respond to real-time threats to 5G/6G connectivity, with established rollback mechanisms for Satcoms during disruptions [111], [69]. Compliance with evolving 5G/6G standards and rigorous security testing in realistic 5G/6G environments are essential [4], [69]. Also, fostering interdisciplinary collaboration between satellite and 5G/6G experts and ensuring compliance with specific regulations related to 5G/6G integration completes the holistic approach to safeguarding the integrated Satcoms-5G/6G environment [4].

Moreover, the emerging 5G and 6G-based non-terrestrial networks that conduct portions of the 5G/6G processing in the satellites [47], [305], [306], [307], [308], [309], [310], [311] pose novel security challenges that need urgent attention. In the context of optical communications [312], [313], [314], [315], it is imperative to address potential vulnerabilities related to signal interception and secure data transmission over optical links [204], [316]. Optical communications, while offering high bandwidth and low latency advantages, may be susceptible to eavesdropping [317], [318], [319] or jamming [320], necessitating robust encryption [321], [322] and authentication [204], [323]. Comprehensive security measures must be implemented to safeguard the confidentiality and integrity of data transmitted through optical channels in these non-terrestrial networks [324], [325], [316], [326].

Regenerative satellites, which conduct extensive onboard 5G/6G signal and protocol processing, introduce complexities in managing and securing these processes, necessitating advanced security measures [327], [328]. The onboard processing capabilities make regenerative satellites potential targets for sophisticated cyberattacks [120], [84], including signal manipulation or protocol exploits. Implementing secure coding practices [69], regular security audits [111], and incorporating IDSs [214] are crucial elements to fortify these regenerative satellites against cyberthreats. Additionally, ongoing research is essential to stay ahead of emerging attack vectors and vulnerabilities specific to regenerative satellite architectures [327].

Furthermore, understanding the intricacies of advanced signal processing within such 5G/6G networks is crucial for identifying and mitigating potential threats [122]. Advanced signal processing techniques, while enhancing the efficiency of 5G/6G networks, may introduce new security challenges. This includes potential vulnerabilities in algorithms, signal manipulation risks, and the need for resilient signal processing architectures [12], [6], [122]. Collaborative efforts between signal processing experts and security professionals are essential to comprehensively address these challenges and to ensure the integrity and reliability of signal processing in non-terrestrial 5G/6G networks.

These multifaceted security considerations underscore the need for proactive research, robust implementation of security protocols, and ongoing vigilance to protect the integrity and confidentiality of data within the evolving landscape of non-terrestrial 5G/6G networks that integrate with satellite communications.

E. Summary and Discussion

This section comprehensively summarized the key lessons learned to enhance the cybersecurity of Satcoms systems. These insights stem from our in-depth analysis of Satcoms cyberattacks and the corresponding cybersecurity strategies in

Sections IV and V. The lessons encompass a multifaceted approach to bolstering Satcoms security, addressing critical aspects, such as attack prevention, attack resilience planning, recovery from attacks, and integration with 5G/6G systems. The central theme emphasizes proactive measures, highlighting the importance of strengthening defenses before threats materialize.

More specifically, the section underscores the paramount importance of attack prevention, emphasizing strict adherence to rigorous regulations and standards, continuous monitoring complemented by threat intelligence, and the adoption of a DiD strategy. Furthermore, it highlights the significance of attack resilience planning, encompassing elements such as identifying a minimal subset of critical components, reducing the attack surface through secure communication channels and access controls, and establishing robust contingency plans. Collectively, these measures increase the chances that Satcoms systems maintain their functionality even in the face of cyberthreats and disruptive events. Additionally, the concept of self-recovery is noted, acknowledging the unique challenges faced by satellite systems, which must autonomously operate over extended periods.

Moreover, the section sheds light on emerging considerations that the integration of Satcoms with 5G/6G systems presents, including network slicing, secure communication protocols, and interdisciplinary collaboration between satellite and 5G/6G experts. These factors are crucial for effectively securing the integrated networks, reflecting the ever-evolving landscape of Satcoms cybersecurity.

VII. Open Challenges for Satcoms Cybersecurity

This section covers the main open challenges faced by Satcoms systems and outlines future research and development directions to address these open challenges. Generally, to provide the degree of service that the users demand, the level of provided security must be judiciously balanced against the usability of a Satcoms system as well as the resource expenditures (e.g., energy, computing cycles, and memory) for the security mechanisms [111]. This balancing principle applies in general to all future research directions that are outlined in this section.

A. *Security and Privacy-related Challenges in Satcoms System*

Satcoms systems present unique security and privacy challenges that necessitate focused research and development [17], [44], [147]. These challenges stem from the intricate interplay between the technological and operational aspects of Satcoms systems [124]. Addressing these challenges is not only critical for safeguarding data and operations but also for ensuring the resilience and effectiveness of satellite-based communication [44], [214], [172].

The crucial open security and privacy challenges in Satcoms systems include ensuring secure communications and lightweight authentication mechanisms [89], managing firmware and software updates effectively [69], [228], addressing scalability and key management issues [49], securing the supply chain [69], and defending against APTs [159], [66].

1) Efficient Secure Communications and Lightweight Authentication:

a) Balancing Security and Efficiency: In light of the state-of-the-art cybersecurity strategies surveyed in the preceding sections, especially in Section V, a notable open challenge emerges within Satcoms systems: the intricate balance between security and efficiency [75], [66]. While the inherent design of Satcoms protocols emphasizes efficiency by minimizing power, memory consumption, and transmission delay, the introduction of robust security measures can potentially introduce substantial overhead that may not align with specific mission requirements [7]. Consequently, striking an optimal balance between security enhancements and mission demands becomes paramount during the design and decision-making phases of any given mission, aiming to establish an acceptable level of risk [12], [66].

To address this challenge, future research and development should formulate lightweight security solutions that seamlessly integrate with mission requisites [69], [44]. Innovative approaches include the integration of hardware security mechanisms directly into the Satcoms hardware [329], the exploration of advanced encryption algorithms that offer heightened security without significant overhead [195], [241], and the development of adaptive security protocols [330] capable of dynamically adjusting security levels in accordance with mission needs. Additionally, focusing on the creation of a comprehensive risk-benefit tradeoff framework is essential, accounting for energy expenditures in fending off potential attacks versus the risks of allowing an attack to progress [331]. This framework can guide satellite operators in informed decision-making by quantitatively analyzing associated risks and benefits [110].

In particular, future research could explore the possibility of allowing relatively benign attacks to proceed in a controlled manner, as a strategy to conserve energy and resources [69], [110]. Such a tactic necessitates the development of novel attack detection and monitoring methods and a deeper comprehension of the trade-offs inherent in disrupting attacks at different stages [75]. Ultimately, the overarching aim is to strike a sensible balance between defensive energy expenditures and the risks of succumbing to severe attacks, while ensuring continuous protection and operation of critical systems [69], [75].

b) Mission-Specific Security: Given the diversity and complexity of Satcoms systems and their mission protocols [26], it is crucial to develop comprehensive frameworks and standards that can categorize missions according to their specific tasks, purposes, and associated security requirements [6], [69]. Such frameworks should take into account the associated risk factors, such as the nature of the data being transmitted, the level of sensitivity or confidentiality required, and the potential consequences of a security breach [110]. Future research should focus on developing and evaluating such frameworks, with the goal of providing clear guidelines for Satcoms operators and industry stakeholders on how to implement secure communication and authentication protocols for different types of missions [24].

Additionally, the frameworks and standards should recommend the appropriate control and communication protocols and mechanisms to be utilized for each type of mission. This will help ensure that the implemented security measures are commensurate with the level of risk associated with each mission, while also enabling greater interoperability and collaboration among Satcoms operators and users [69], [24].

c) Physical Layer Security: Acknowledging that prevailing Satcoms protocols often prioritize functionality over security, thereby exposing vulnerabilities that can be exploited by attackers [44], [23], it is imperative to explore alternatives. While computational cryptographic methodologies are conventionally employed for encryption, they may not uniformly suffice against advanced attacks [69]. To this end, future research should explore the potential of physical layer security [332], [333], [334], [69] as an alternative or complement to cryptographic protocols in Satcoms.

Physical layer security exploits the unique physical properties of the wireless channel to provide security, making it resistant to attacks that rely on computational strategies [16], [66]. By leveraging physical layer security, Satcoms can enhance their overall security posture and ensure resilience against a wide range of threats [69].

The integration of physical layer security holds particular allure for embedded systems, such as CubeSats, which face limitations in power consumption and code space for computational cryptographic calculations [288]. Embracing physical layer security mechanisms, such as artificial noise [335], jamming [16], and beamforming [336], exploits the inherent unpredictability of wireless channels to achieve security. Nevertheless, it is imperative that significant future research and development efforts are dedicated to maturing physical layer security into a dependable component of Satcoms systems' overarching cybersecurity framework [337], [338], [339]. This progress will ensure the steadfastness and effectiveness of security measures across the intricate fabric of Satcoms systems [204].

2) Effective Firmware and Software Updates: Firmware and software updates in Satcoms systems continue to pose several main challenges [36], [69]:

- Limited bandwidth: Satellites often grapple with constrained bandwidth, which can slow down and complicate the transmission of software and firmware updates [122]. Even relatively modest updates may require a substantial amount of time for transmission to and reception by the satellite [69].
- Remote location: The remoteness of satellites can exacerbate difficulties in diagnosing and resolving issues that may arise during or after an update [111].
- Reliability considerations: Satellites are designed to be highly reliable and to operate for long periods of time without failure. However, software and firmware updates can introduce new risks and potential points of failure, which can be difficult to mitigate [24].
- Security implications: Updates involving software, firmware, hardware, or cryptographic keys can inadvertently introduce novel vulnerabilities that could be exploited by malicious actors [155], [69]. Ensuring the security of updates can be a major challenge, especially given the limited bandwidth and remote location of satellites [261].
- Compatibility challenges: Satellites often use complex and specialized software and firmware that may not be compatible with the latest technologies or standards [158]. Consequently, updating these systems can be difficult and may require significant testing and validation to ensure compatibility with other systems [24].

These challenges necessitate careful planning, testing, and monitoring to ensure that software and firmware updates are implemented safely and effectively [158], [261]. One promising approach could be to build on newly emerging technologies, such as software attestation [46] and virtualization [124], [300] to help address these challenges.

Future research should be directed toward the development, evaluation, and validation of detailed protocol mechanisms for firmware and software updates in Satcoms systems [69]. Through innovation in this context of firmware and software update protocols, it may be possible to address the challenges surrounding firmware and software updates more effectively, with the goal of ensuring the continued operational resilience of Satcoms systems [66], [124].

3) Scalability and Effective Key Management:

a) Scalability Challenges: Scalability and key management represent pivotal challenges within Satcoms systems that necessitate tailored solutions [49]. As these systems accommodate a growing number of users and devices, they encounter escalating demands for network traffic, performance, and reliability [340]. Ensuring seamless scalability while maintaining robust security mechanisms demands a nuanced approach [69], [66]. Furthermore, effective key management is imperative to secure communications in Satcoms systems [49]. While scaling up the system, distributing and updating cryptographic keys across diverse devices becomes complex and resource-intensive [69]. The need for secure and efficient key distribution, rotation, and storage underscores the necessity of optimization techniques [341], [66].

b) Optimization Techniques: To effectively address these challenges, the strategic application of optimization techniques [279] can streamline the scalability of Satcoms systems [111]. Leveraging algorithms designed to enhance resource allocation, load balancing, and network utilization can effectively alleviate congestion and sustain high system performance as the user base expands [69]. Moreover, harnessing optimization-driven solutions can automate key management processes, ensuring secure generation, distribution, and rotation of cryptographic keys [66], [279]. These strategies can not only bolster security but can also significantly reduce the operational overhead associated with manual key management [49].

c) Synergistic Scalable Key Management: In the context of large and complex systems, such as Satcoms networks, where key management is inherently challenging, it is important to note that effective key management need not impede scalability [6], [66]. On the contrary, the key management can synergistically support scalability by enabling secure key sharing across multiple devices and users [69]. Such a synergistic approach can mitigate the overhead linked to managing individual keys for each user or device, thereby streamlining system administration. A detailed exploration of this dynamic interplay necessitates further investigation in future research [49].

d) Quantum Key Distribution: Furthermore, future research should thoroughly explore emerging key management technologies, such as quantum key distribution [341], and investigate how quantum key distribution can address the key management challenges in Satcoms systems [49]. This innovative approach leverages the principles of quantum mechanics to establish secure communication channels, providing enhanced security and potentially revolutionizing key management practices in Satcoms systems. By embracing quantum key distribution, Satcoms systems could overcome the limitations of traditional cryptographic key exchange methods and establish a stronger foundation for secure communication [49], [69].

4) Supply Chain Security: While there has been significant attention paid to cyberattacks on Satcoms supply chains [24], there has been relatively little specific focus on strategies that address the risks associated with supply chain security for Satcoms systems [69], [28]. This has resulted in several critical open challenges that need to be addressed in future research and development [12], [28]. The main open challenges related to supply chain security for Satcoms systems include:

- Limited visibility: The Satcoms supply chain involves many vendors and suppliers, making it inherently challenging to gain comprehensive visibility into the security practices of each entity [12], [69].
- Lack of transparency and traceability: The complexity of Satcoms supply chains poses difficulties in effectively tracking and monitoring all components. This challenge impedes the identification and mitigation of potential vulnerabilities [152], [69].
- Threat of malicious components: The incorporation of counterfeit or malicious components within Satcoms systems introduces vulnerabilities, escalating the risk of cyberattacks [15], [69].
- Third-party software vulnerabilities: Satcoms systems often rely on third-party software components, which can introduce vulnerabilities if not properly vetted [111].
- Integration complexity: The integration of components from multiple vendors can be challenging, particularly if security controls are not properly implemented [12].
- Navigating complex logistics: Satcoms systems involve complex logistics, and it can be challenging to ensure that all components are properly secured throughout the supply chain [20], [69].
- Cost and resource constraints: The implementation of supply chain security measures often demands substantial financial and resource investments, especially for smaller organizations [15], [69].

Addressing these open challenges mandates the development of comprehensive supply chain security frameworks that ensure transparency and traceability across the entire Satcoms system supply chain [28], [24]. This can be achieved through the adoption of advanced tracking and authentication technologies, thereby validating the authenticity and integrity of components [69]. Additionally, forging partnerships with trusted suppliers and vendors may reduce the vulnerability to supply chain compromises [12], [24].

Effectively addressing these open challenges in supply chain security holds the key to guaranteeing the sustained security and reliability of Satcoms systems [69], [24]. By doing so, Satcoms operators can proactively mitigate the risks associated with the intricate and globally distributed Satcoms supply chains, thus ensuring the delivery of secure and dependable services to their users and customers [139].

5) Addressing Advanced Persistent Threats (APTs): APTs are long-term, targeted cyberattacks that are designed to remain undetected for extended periods of time [159]. APTs are typically carried out by well-resourced and highly-skilled attackers, such as nation-state actors or organized crime groups, and they are often focused on stealing sensitive information or disrupting critical infrastructure [15], [66]. Within the context of Satcoms systems, beyond the stealthy nature of those threats, APTs pose distinct challenges that require focused attention [159]:

- High-value targets: Satcoms systems frequently underpin critical infrastructure, encompassing military, transportation, and emergency services [98], [99], [17]. Their pivotal role renders them attractive to APTs driven by political, economic, or strategic motives [12], [66].
- Resource-intensive response: Effectively countering APTs demands substantial resources, including advanced threat detection and response capabilities, as well as extensive knowledge of an organization's Satcoms systems and operations [16].
- Evolving Threat Landscape: APTs are continually evolving, driven by the attackers' quest for novel methods to bypass defenses and access sensitive information. Keeping pace with these dynamic threats presents a significant challenge for the security of Satcoms systems [159].

Future research must focus on the development and evaluation of sophisticated, adaptive security strategies capable of mitigating the evolving threats posed by APTs [15], [159]. Leveraging ML and AI techniques can substantially enhance APT identification and mitigation capabilities [38], [39]. Striking a balance between the efficacy of the defense mechanisms against APTs and the associated costs, such as energy consumption and computational resources, is paramount [66]. [66]. As such, future research should concentrate on creating energy-efficient and resource-conscious security solutions capable of sustaining a persistent defense against the persistent nature of APTs threats [111].

Additionally, establishing standardized best practices and protocols for APTs defense within Satcoms systems is crucial [66]. This standardization ensures interoperability and facilitates the seamless adoption of these security strategies across diverse Satcoms systems and vendors, enhancing the collective resilience of the Satcoms ecosystem [69].

B. Throughput and Energy Consumption

Throughput refers to the amount of data that can be transmitted during a given time period. In Satcoms, higher throughput means that more data can be transmitted between two or more satellites, resulting in more efficient and faster communication [41]. However, increased throughput also introduces challenges, particularly with inter-satellite links. Inter-satellite links are the connections between two or more satellites, and play a critical role in enabling high-speed data transfer [56].

Managing inter-satellite links requires careful power control, as well as a proper understanding of link budgets and system complexities [342]. Link budget refers to the calculation of the power required to establish and maintain a communication link between two satellites, while system complexity refers to the level of complexity involved in setting up and managing the inter-satellite links [342]. Ensuring that inter-satellite links are established and maintained efficiently while minimizing power consumption requires careful consideration of these factors [66]. Therefore, future research should focus on developing and evaluating link budget optimization techniques that enable Satcoms systems to operate at maximum efficiency while minimizing power consumption [66].

Another challenge that affects throughput is interference from other systems. This interference can reduce the throughput and should be addressed by interference mitigation techniques, such as frequency allocation and power control [56], [343]. Frequency allocation assigns specific frequency bands to Satcoms systems to prevent interference from other communication systems.

Power control regulates the transmission power of Satcoms systems to minimize interference with other communication systems. As the satellite industry transitions to New Space, the frequency bands become more crowded, making interference management and power control more complicated [28]. Additionally, as Satcoms systems continue to increase in throughput, there is a need for more efficient power management techniques to minimize energy consumption and extend the operational life of satellites. Therefore, future research should focus on developing and evaluating new power management and interference mitigation techniques that effectively manage these challenges in the context of New Space [28], [66].

Energy efficiency is also an important concern for Satcoms systems [56]. Since satellites rely on limited power sources, such as solar panels, it is critical to design energy-efficient communication protocols and power management strategies. These strategies can help to minimize power consumption while maximizing the efficiency of the data transfer between satellites [69]. This can be achieved through the use of low-power components and optimizing the communication protocols to reduce the number of transmissions required for each data transfer [19]. Another promising approach to achieving energy efficiency in Satcoms systems is the use of hardware acceleration modules [344], [345]. These modules are specialized hardware components that are designed to perform specific computations more efficiently than traditional software-based methods. By outsourcing certain computations to these hardware modules, Satcoms systems can reduce the amount of energy required to perform those computations and, in turn, improve their energy efficiency.

Balancing these competing demands is critical to provide the degree of service that users desire. Therefore, careful consideration must be given to security and usability concerns during the design and decision-making phases of Satcoms missions to establish an acceptable risk level. Furthermore, the fulfillment of these competing demands needs to be rigorously evaluated, whereby the evaluations should involve testbeds to account for the full range of effects occurring in real Satcoms systems [346], [347].

C. *Regulatory Compliance*

Satcoms systems are subject to a variety of regulations [15]. Compliance with these regulations can be complex and challenging, particularly for organizations operating in multiple countries [12], [69]. The challenges related to regulatory compliance in Satcoms systems include:

- Understanding and interpreting complex regulations: Satcoms systems are subject to a range of regulations, which can be difficult to understand and interpret, particularly for organizations operating in multiple countries with different regulations [348].
- Maintaining compliance with changing regulations: Regulations are often updated or revised, and organizations must ensure that their Satcoms systems remain compliant with these changes [12].
- Meeting multiple regulatory requirements: Satcoms must comply with a variety of regulations, including those related to security, privacy, and export controls [15].
- Ensuring compliance across the supply chain: Satcoms are complex and involve many different components and vendors. Ensuring compliance across the entire supply chain can be difficult, particularly for organizations with limited visibility into the security practices of their suppliers [12].
- Addressing the cost of compliance: Compliance with regulations can be expensive, particularly for smaller organizations with limited resources. The cost of compliance may include investments in technology, personnel, and third-party audits [348].
- Managing international regulations: Organizations operating in multiple countries must comply with the regulations of each country in which they operate, which can be complex and challenging [12], [69].
- Ensuring compliance with data protection regulations: Satcoms systems often involve the processing and transmission of sensitive data [36] and must comply with data protection regulations such as the General Data Protection Regulation (GDPR) [209] in Europe.

Overall, regulatory compliance is a significant challenge for Satcoms systems, requiring ongoing attention and investment to ensure that they are meeting legal and ethical obligations [348], [20].

D. *Limited Resources*

Limited resources can be a significant challenge for Satcoms systems in terms of regulatory compliance as well as cybersecurity [272]. It can be difficult for organizations with limited resources to allocate the necessary time, budget, and personnel to ensure compliance with complex regulations and to implement effective cybersecurity measures [39], [69]. This can leave these systems vulnerable to attacks and potentially unable to meet compliance requirements, which can result in legal and financial consequences [348]. Additionally, the constantly evolving threat landscape means that organizations need to regularly update their cybersecurity measures, which can be difficult for those with limited resources [121], [69]. The main challenges related to limited resources in Satcoms systems are:

- Lack of funding: Organizations may not have the necessary funding to invest in robust cybersecurity measures, leaving them vulnerable to cyberattacks [15].
- Limited staff: Small organizations may not have the resources to hire dedicated cybersecurity staff, which can make it difficult to manage and respond to security incidents [348].
- Outdated equipment: Organizations with limited resources may be using outdated equipment that is more vulnerable to cyberattacks and harder to secure [12].
- Lack of training: Staff may not have the necessary training and awareness to identify and respond to security incidents [24].
- Inadequate risk assessments: Organizations may not have the resources to conduct thorough risk assessments and implement appropriate security controls [289].
- Inability to keep up with emerging threats: Limited resources may make it difficult to stay up to date with the latest threats and implement appropriate security measures [159].

The emergence of New Space companies, particularly those with a for-profit model, has intensified the competition and drive to reduce costs in the satellite industry [28]. This exacerbates the scarcity of resources available for implementing appropriate security measures and keeping up with emerging threats. As companies try to cut costs, security measures may be seen as an unnecessary expense, leaving satellite systems vulnerable to cyberattacks and other security risks.

E. Novel Communication Paradigms

The emergence of novel communication paradigms may open entirely new avenues for ensuring the cybersecurity of Satcoms systems. One prominent emerging paradigm in the context of Satcoms is quantum-based communication [340], [349], [350], [351], [352]. The novel quantum-based communication mechanisms may facilitate entirely novel quantum-based cybersecurity mechanisms [353], [354], [355], [356] that need to be thoroughly investigated in future research.

Also, the emerging Beyond Shannon communication paradigms broaden the communications problem from the traditionally considered technical problem of replicating the information at the sender with as few errors as possible at a distant receiver to the consideration of the semantic and effectiveness problems [357], [358]. Emerging semantic communication strategies, see e.g., [359], [360], [361], [362], [363], strive to convey not the entire set of source information, but rather only the semantic meaning that is represented by the source information. Aside from potentially achieving substantial compression gains, semantic communication has the potential to enable novel security strategies [364], [365], [203], [366] that should be explored and evaluated in the context of Satcoms systems in future research.

Similarly, communication paradigms that operate at the effectiveness level [357], [358], such as identification via channels [367], [368], [369], [370] may facilitate efficient secure communications for particular goal-oriented purposes in Satcoms systems. Identification via channels does not convey the information from the source to the destination, but rather verifies whether sets of information at the source and the destination are identical or not. Communication tasks that verify synchronization between distant components, e.g., in digital twin settings [224], [371], [372], [373] could be carried out highly efficiently with identification via channels. Also, identification coding may provide an effective alternative to hash functions, e.g., in secure hash function applications for encryption.

Due to the specific information-theoretic properties of the identification via channels approach, the required communication bitrate can be reduced on an exponential scale compared to conventional technical-level communication and entirely novel security mechanisms can be exploited [374], [375]. Both digital twin-based techniques for controlling and operating satellite networks [376], [377], including their cybersecurity aspects [223], as well as the potential of secure Satcoms communication via the identification via channels paradigm should be explored and evaluated in future research.

Network coding [378], [379], [380], [381] has extended the conventional store-and-forward packet transport paradigm to a store-recode-forward paradigm that enhances the transport capacity of networks. The basic principle of network coding can substantially enhance satellite network services [382], [383]. Also, network coding offers attractive cybersecurity properties [384], [385], [386] that need to be thoroughly investigated in the context of Satcoms systems, where satellites could carry out the recoding onboard. While network coding is generally computationally demanding, so-called sparse network coding approaches [387], [388], [389], [390] can substantially reduce the computational complexity. Future research needs to comprehensively examine these sparse network coding approaches and their tradeoffs, e.g., how much throughput and security loss is incurred for increasing levels of sparsity [69], [70].

VIII. Conclusion

Satcoms systems are becoming increasingly important in today's interconnected world. With the growing reliance on satellite technology, the cybersecurity of Satcoms has become a critical concern since cyberattacks on Satcoms can have significant consequences, from loss of communication to the disclosure of sensitive data. This survey first reviewed the Satcoms architecture, including the space segment, the ground segment, and the links segment.

Following the classification according to the Satcoms system segments, we have then comprehensively surveyed the cyberattacks on Satcoms systems as well as the cybersecurity strategies to defend Satcoms systems against cyberattacks.

Specifically, for the three major segments of Satcoms systems, namely the ground segment, the space segment, and the links segment, we have comprehensively surveyed the respective cyberattacks and cybersecurity techniques. Within each segment, we have developed taxonomy schemes for the Satcoms-specific cyberattacks and cybersecurity strategies. We have also classified the various types of potential attackers who may target Satcoms systems while emphasizing the significant consequences that cyberattacks can have on Satcoms systems. These consequences highlight the critical importance of Satcoms cybersecurity, as cyberattacks can cause disruption of communication services, breach of sensitive data, physical damage to satellites, GPS jamming and spoofing, and even cyberwarfare.

Furthermore, we have synthesized the main learned lessons derived from the extensive survey of cyberattacks and cybersecurity strategies within the context of Satcoms systems. We have also outlined the main open challenges that persist in this domain, alongside the corresponding avenues for future research. Thus, this survey has provided a comprehensive view of the evolving landscape of cybersecurity in Satcoms systems.

ACKNOWLEDGEMENT

This work has been supported by the SmartSat CRC (RG214317), whose activities are funded by the Australian Government's CRC Program. It has also been supported by the Australian Research Council / Discovery Early Career Researcher Award, DE23010011.

REFERENCES

[1] A. de Concini, J. Toth, and S. Dustdar, "The future of the European space sector," 2020. [Online]. Available: https://www.eib.org/attachments/thematic/future_of_european_space_sector_en.pdf

[2] "ESA Facts - European Space Agency," 2022. [Online]. Available: https://www.esa.int/About_Us/Corporate_news/ESA_facts

[3] K. Mai'a, "Space security and the transatlantic relationship," *Politics and Governance*, vol. 10, no. 2, pp. 134–143, 2022.

[4] S. Chen, S. Sun, and S. Kang, "System integration of terrestrial mobile communication and satellite communication—the trends, challenges and key technologies in B5G and 6G," *China Communications*, vol. 17, no. 12, pp. 156–171, 2020.

[5] A. Guidotti, S. Cioni, G. Colavolpe, M. Conti, T. Foggi, A. Mengali, G. Montorsi, A. Piemontese, and A. Vanelli-Coralli, "Architectures, standardisation, and procedures for 5G satellite communications: A survey," *Computer Networks*, vol. 183, Art. no. 107588, 2020.

[6] O. Kodheli, et al., "Satellite communications in the new space era: A survey and future challenges," *IEEE COMST*, vol. 23, no. 1, pp. 70–109, 2020.

[7] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao, and J. Shi, "Broadband LEO satellite communications: Architectures and key technologies," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 55–61, 2019.

[8] C. Niephaus, M. Kretschmer, and G. Ghinea, "QoS provisioning in converged satellite and terrestrial networks: A survey of the state-of-the-art," *IEEE COMST*, vol. 18, no. 4, pp. 2415–2441, 2016.

[9] N. Saeed, A. Elzanaty, H. Almorad, H. Dahrouj, T. Y. Al-Naffouri, and M.-S. Alouini, "CubeSat communications: Recent advances and future challenges," *IEEE COMST*, vol. 22, no. 3, pp. 1839–1862, 2020.

[10] B. M. Esiefarienrhe and T. Moemi, "Satellite: A tool to enhance a country's security and economic development," *African Journal of Development Studies*, vol. 2023, no. si2, pp. 207–218, 2023.

[11] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels cybersecurity: Issues, challenges, and the road ahead," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 90–96, 2020.

[12] B. Bailey, R. Speelman, P. Doshi, N. Cohen, and W. Wheeler, "Defending spacecraft in the cyber domain," Nov. 2019. [Online]. Available: https://csps.aerospace.org/sites/default/files/2021-08/Bailey_DefendingSpacecraft_11052019.pdf

[13] J. Chu, X. Chen, C. Zhong, and Z. Zhang, "Robust design for NOMA-based multibeam LEO satellite internet of things," *IEEE Internet of Things journal*, vol. 8, no. 3, pp. 1959–1970, 2020.

[14] S. S. Sefati and S. Halunga, "Ultra-reliability and low-latency communications on the internet of things based on 5G network: Literature review, classification, and future research view," *Trans. on Emerging Telecommun. Techn.*, Art. no. e4770, 2023.

[15] L. Shadbolt, *Technical Study Satellite Cyberattacks and Security*. HDI Global SE, Australia, 2021. [Online]. Available: https://www.hdi.global/infocenter/insights/specialty/technical-study/

[16] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *International Journal of Information Security*, vol. 20, no. 3, pp. 287–311, 2021.

[17] H. Lueschow and R. Pelaez, "Satellite communication for security and defense," *Handbook of Space Security: Policies, Applications and Programs*, pp. 779–796, 2020.

[18] "Ukraine: A timeline of cyberattacks, cyberpeace institute 2022," 2022, (Accessed on 06/09/2022). [Online]. Available: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

[19] S. L, "Technical study: Satellite cyberattacks and security," June 2021. [Online]. Available: https://www.hdi.global/infocenter/insights/specialty/technical-study/

[20] J. Black, L. Slapakova, and K. Martin, *Future Uses of Space Out to 2050: Emerging threats and opportunities for the UK National Space Strategy*. Santa Monica, CA: RAND Corporation, 2022.

[21] D. Livingstone and P. Lewis, *Space, the Final Frontier for Cybersecurity?* Chatham House, The Royal Institute of International Affairs, London, UK., 2016.

[22] D. Paikowsky, "What is new space? The changing ecosystem of global space activity," *New Space*, vol. 5, no. 2, pp. 84–88, 2017.

[23] A. Nassisi and I. Patatti, "Space systems and space sovereignty as a security issue," *Handbook of Space Security: Policies, Applications and Programs*, pp. 211–226, 2020.

[24] B. Sawik, "Space mission risk, sustainability and supply chain: Review, multi-objective optimization model and practical approach," *Sustainability*, vol. 15, no. 14, Art. no. 11002, 2023.

[25] A. C. Skelton, "Vulnerabilities in satellite communications underscore threat to critical infrastructure," INL/RPT-23-73517-Rev000, Idaho National Laboratory (INL), Idaho Falls, ID, Tech. Rep., 2023.

[26] T. Llanso and D. Pearson, "Achieving space mission resilience to cyber attack: Architectural implications," in *AIAA SPACE*. American Institute of Aeronautics and Astronautics, California, 2016, Paper no. 5604.

[27] "State of the satellite industry report," 2021. [Online]. Available: https://brycetech.com/reports

[28] R. Graczyk, P. Esteves-Verissimo, and M. Voelp, "Sanctuary lost: A cyber-physical warfare in space," *arXiv preprint arXiv:2110.05878*, 2021.

[29] D. Housen-Couriel, "Cybersecurity threats to satellite communications: Towards a typology of state actor responses," *Acta Astronautica*, vol. 128, pp. 409–415, 2016.

[30] A. A. Z. Hudaib, "Satellite network hacking & security analysis," *International Journal of Computer Science and Security (IJCSS)*, vol. 10, no. 1, pp. 8–55, 2016.

[31] L.-A. Turner and H. Jahankhani, "An investigation into an approach to updating the governance of satellite communications to enhance cyber security," in *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proc. 13th Int. Conf. on Global Security, Safety and Sustainability*. Springer, Cham, 2021, pp. 23–33.

[32] L. Vessels, K. Heffner, and D. Johnson, "Cybersecurity risk assessment for space systems," in *Proc. IEEE Space Computing Conference (SCC)*, 2019, pp. 11–19.

[33] D. P. Fidler, "Cybersecurity and the New Era of Space Activities, Maurer School of Law, Indiana Univ., Bloomington," 2018.

[34] M. Scholl and T. Suloway, "Introduction to cybersecurity for commercial satellite operations, NISTIR 8270," U.S. National Institute of Standards and Technology (NIST), Tech. Rep., Feb. 2022.

[35] G. Falco, "Cybersecurity principles for space systems," *Journal of Aerospace Information Systems*, vol. 16, no. 2, pp. 61–70, 2019.

[36] D. He, X. Li, S. Chan, J. Gao, and M. Guizani, "Security analysis of a space-based wireless network," *IEEE Network*, vol. 33, no. 1, pp. 36–43, 2019.

[37] G. Falco, "When satellites attack: Satellite-to-satellite cyber attack, defense and resilience," in *ASCEND 2020*. Aerospace Research Central, 2020, pp. 4014:1–4014:9. [Online]. Available: https://arc.aiaa.org/doi/abs/10.2514/6.2020-4014

[38] M. Rath and S. Mishra, "Security approaches in machine learning for satellite communication," in *Machine Learning and Data Mining in Aerospace Technology*. Springer, Cham, 2020, pp. 189–204.

[39] F. Fourati and M.-S. Alouini, "Artificial intelligence for satellite communication: A review," *Intelligent and Converged Networks*, vol. 2, no. 3, pp. 213–243, 2021.

[40] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in *AIAA Scitech Forum*, 2021, Paper no. 0773.

[41] C. Wang, Z. Zhang, J. Wu, C. Chen, and F. Gao, "An overview of protected satellite communications in intelligent age," *Science China Information Sciences*, vol. 64, no. 6, pp. 1–18, 2021.

[42] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity challenges in the maritime sector," *Network*, vol. 2, no. 1, pp. 123–138, 2022.

[43] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, Art. no. 22, 2022.

[44] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, Art. no. 109246, 2022.

[45] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE COMST*, vol. 25, no. 3, pp. 1604–1652, 2023.

[46] Q. Wang, X. Chen, X. Jin, X. Li, D. Chen, and X. Qin, "Enhancing trustworthiness of internet of vehicles in space–air–ground-integrated networks: Attestation approach," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5992–6002, 2021.

[47] M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, J. F. Mendoza Montoya, S. Pollin, A. Haqiqatnejad, A. Mostaani, E. Lagunas, and B. Ottersten, "Evolution of non-terrestrial networks from 5G to 6G: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 4, pp. 2633–2672, 2022.

[48] N.-N. Dao, Q.-V. Pham, N. H. Tu, T. T. Thanh, V. N. Q. Bao, D. S. Lakew, and S. Cho, "Survey on aerial radio access networks: Toward a comprehensive 6G access infrastructure," *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 2, pp. 1193–1225, 2021.

[49] 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 & Tutorials*, vol. 24, no. 1, pp. 53–87, 2021.

[50] B. Tezergil and E. Onur, "Wireless backhaul in 5G and beyond: Issues, challenges and opportunities," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 4, pp. 2579–2632, 2022.

[51] D. Zhou, M. Sheng, J. Li, and Z. Han, "Aerospace integrated networks innovation for empowering: A survey and future challenges," *IEEE Commun. Surv. & Tut.*, vol. 25, no. 2, pp. 975–1019, 2023.

[52] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Commun. Surv. & Tut.*, vol. 23, no. 3, pp. 1693–1720, 2021.

[53] H. Al-Hraishawi, H. Chougrani, S. Kisseleff, E. Lagunas, and S. Chatzinotas, "A survey on nongeostationary satellite systems: The communication perspective," *IEEE Commun. Surveys & Tutorials*, vol. 25, no. 1, pp. 101–132, 2023.

[54] A. Grenier, E. S. Lohan, A. Ometov, and J. Nurmi, "A survey on low-power GNSS," *IEEE COMST*, vol. 25, no. 3, pp. 1482–1509, 2023.

[55] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE COMST*, vol. 20, no. 4, pp. 2714–2741, 2018.

[56] R. Radhakrishnan, W. W. Edmonson, F. Afghah, R. M. Rodriguez-Osorio, F. Pinto, and S. C. Burleigh, "Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view," *IEEE COMST*, vol. 18, no. 4, pp. 2442–2473, 2016.

[57] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE COMST*, vol. 24, no. 1, pp. 160–209, 2022.

[58] M. Husak, J. Komarkova, E. Bou-Harb, and P. Celeda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019.

[59] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 4, pp. 2525–2556, 2021.

[60] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, pp. 1744–1772, 2019.

[61] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on iot networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 1, pp. 248–279, 2022.

[62] E. Rodríguez, B. Otero, N. Gutiérrez, and R. Canal, "A survey of deep learning techniques for cybersecurity in mobile networks," *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 3, pp. 1920–1955, 2021.

[63] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE COMST*, vol. 24, no. 3, pp. 1475–1503, 2022.

[64] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE COMST*, vol. 22, no. 3, pp. 1942–1976, 2020.

[65] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5G enabled internet-of-medical-things," *IET Communications*, vol. 16, no. 5, pp. 421–432, 2022.

[66] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[67] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2019.

[68] G. Nencioni, R. G. Garroppo, and R. F. Olimid, "5G multi-access edge computing: A survey on security, dependability, and performance," *IEEE Access*, vol. 11, pp. 63 496–63 533, 2023.

[69] S. O. Oruma and S. Petrović, "Security threats to 5G networks for social robots in public spaces: A survey," *IEEE Access*, vol. 11, pp. 63 205–63 237, 2023.

[70] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Security and Privacy*, vol. 6, no. 1, Art. no. e271, 2023.

[71] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, Art. no. 107345, 2020.

[72] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, Art. no. 1969, 2022.

[73] Z. M. Fadlullah, B. Mao, and N. Kato, "Balancing QoS and security in the edge: Existing practices, challenges, and 6G opportunities with machine learning," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 4, pp. 2419–2448, 2022.

[74] X. Lu, L. Xiao, P. Li, X. Ji, C. Xu, S. Yu, and W. Zhuang, "Reinforcement learning-based physical cross-layer security and privacy in 6G," *IEEE Commun. Surv. & Tut.*, vol. 25, no. 1, pp. 425–466, 2023.

[75] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Commun. Surv. & Tut.*, vol. 25, no. 2, pp. 1095–1127, 2023.

[76] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1196–1217, 2023.

[77] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, Art. no. 109515, 2023.

[78] A. A. Elmarady and K. Rahouma, "Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment," *IEEE Access*, vol. 9, pp. 143 997–144 016, 2021.

[79] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, "A survey on cyber security threats in IoT-enabled maritime industry," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2677–2690, 2023.

[80] J. P. Thebarge, W. Henry, and G. Falco, "Developing scenarios supporting space-based IDS," in *ASCEND 2022*. Aerospace Research Central, Las Vegas, Nevada, 2022, pp. 4219:1–4219:12. [Online]. Available: https://arc.aiaa.org/doi/abs/10.2514/6.2022-4219

[81] R. Xu, Y. Chen, E. Blasch, A. Aved, G. Chen, and D. Shen, "Hybrid blockchain-enabled secure microservices fabric for decentralized multi-domain avionics systems," in *Proc. SPIE Sensors and Systems for Space Applications XIII*, vol. 11422, 2020, pp. 150–164.

[82] S. Cao, S. Dang, Y. Zhang, W. Wang, and N. Cheng, "A blockchain-based access control and intrusion detection framework for satellite communication systems," *Computer Communications*, vol. 172, pp. 216–225, 2021.

[83] R. Akeela and B. Dezfouli, "Software-defined radios: Architecture, state-of-the-art, and challenges," *Computer Communications*, vol. 128, pp. 106–125, 2018.

[84] T. Pratt and J. E. Allnutt, *Satellite Communications*. John Wiley & Sons, Hoboken, NJ, 2019.

[85] A. Eskandari and A. Kheirdoost, "Compact and narrow-band waveguide filters using TM dual-mode cavities for input multiplexer in communication satellites," in *Proc. 10th International Symposium on Telecommunications (IST)*, 2020, pp. 234–239.

[86] M. Arslan, "Cybersecurity threats to satellite communications," Dec 2020. [Online]. Available: https://medium.datadriveninvestor.com/cybersecurity-threats-to-satellite-communications-b35d83681723

[87] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Advances in Space Research*, vol. 66, no. 1, pp. 176–192, 2020.

[88] Y. Zheng, T. Mo, D. Wang, W. Wu, Y. Zhao, and Q. Fu, "Research on data encryption technology of power satellite IoT based on IPK," in *Proc. SPIE Third Int. Conf. on Digital Signal and Computer Commun. (DSCC)*, vol. 12716, 2023, pp. 369–377.

[89] S. J. H. Pirzada, T. Xu, and L. Jianwei, "Optimized authentication algorithm on FPGA for space-air-ground integrated network," in *Proc. 14th Int. Conf. on Open Source Sys. and Techn. (ICOSST)*, 2020, pp. 1–6.

[90] G. Oligeri, S. Sciancalepore, S. Raponi, and R. Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Trans. on Inform. Forensics and Sec.*, vol. 18, pp. 274–289, 2022.

[91] M. Tian, F. Li, K. Geng, W. Kou, and C. Guo, "A certificateless conditional anonymous authentication scheme for satellite internet of things," in *Proc. Int. Conf. on Information and Commun. Sec.* Springer, Singapore, 2023, pp. 284–301.

[92] Y. Yang, J. Cao, R. Ma, L. Cheng, L. Chen, B. Niu, and H. Li, "FHAP: Fast handover authentication protocol for high-speed mobile terminals in 5G satellite–terrestrial-integrated networks," *IEEE Internet of Things Journal*, vol. 10, no. 15, pp. 13 959–13 973, 2023.

[93] S. Xu, X. Liu, M. Ma, and J. Chen, "An improved mutual authentication protocol based on perfect forward secrecy for satellite communications," *International Journal of Satellite Communications and Networking*, vol. 38, no. 1, pp. 62–73, 2020.

[94] B. D. Watts, *The Military Use of Space: A Diagnostic Assessment*. Center for Strategic and Budgetary Assessm., Washington, DC, 2001.

[95] G. Furano, G. Meoni, A. Dunne, D. Moloney, V. Ferlet-Cavrois, A. Tavoularis, J. Byrne, L. Buckley, M. Psarakis, K.-O. Voss *et al.*, "Towards the use of artificial intelligence on the edge in space systems: Challenges and opportunities," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 12, pp. 44–56, 2020.

[96] "Number of satellites in orbit by operating country 2022," 2022. [Online]. Available: https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/

[97] "Strand-1 smartphone cubesat_2022," 2022. [Online]. Available: https://amsat-uk.org/satellites/tlm/strand-1/

[98] S. G. Jones, *Three Dangerous Men: Russia, China, Iran and the Rise of Irregular Warfare*. WW Norton & Company, United States, 2021.

[99] "The militarization of space and its transformation into a warfighting domain," 2020. [Online]. Available: https://www.spf.org/iina/en/articles/nagashima_02.html

[100] T. Iida, *Satellite Communications: System and Its Design Technology*. IOS Press, Netherlands, 2000.

[101] E. A. Jerde, "Chapter 2 - the Apollo program," in *Sample Return Missions*. Elsevier, Cambridge, 2021, pp. 9–36. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128183304000021

[102] U. E. Botezatu and O. Bucovetchi, "Space traffic management-key issue for industry 4.0," in *Proc. 10th Int. Conf. on Manufacturing Science and Education*, vol. 343, 2021, pp. 1–9.

[103] R. Rugani, F. Martelli, M. Martino, and G. Salvadori, "Moon village: main aspects and open issues in lunar habitat thermoenergetics design. a review," in *Proc. IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, 2021, pp. 1–6.

[104] L. C. C. P. Mulder and J. T. Siegel, "The future of security in space: A thirty-year US strategy," https://www.atlanticcouncil.org/wp-content/uploads/2021/04/TheFutureofSecurityinSpace.pdf, Apr. 2021.

[105] K. Bernsmed, C. Fr, P. H. Meland, T. A. Myrvoll *et al.*, "Security requirements for SATCOM datalink systems for future air traffic management," in *Proc. IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, 2017, pp. 1–10.

[106] Federal Information Processing Standard (FIPS), "Publication 199. Standards for security categorization of federal information and information systems," *Computer Sec. Div., Inform. Techn. Lab., Nat. Inst. of Standards and Techn., Gaithersburg, MD*, 2004.

[107] S. La Barbera, L. Pighetti, D. Fernandez, M. Admella, and J. G. Cano, "SESAR satcom system identification and verification strategy," in *Proc. IEEE/AIAA 34th Dig. Avionics Sys. Conf.*, 2015, Paper no. 9B4–1.

[108] M. N. Danish, S. A. Pasha, and A. J. Hashmi, "Prototype design of a software-defined radio based SATCOM modem," in *Proc. IEEE Aerospace Conference (50100)*, 2021, pp. 1–7.

[109] A. Jha, B. J. Rao, R. K. Bhan, P. K. Nath, C. V. N. Rao, R. Jyoti *et al.*, "Ka-band FMCW radar altimeter for navigation," in *Proc. IEEE Int. Conf. for Advancement in Techn. (ICONAT)*, 2022, pp. 1–5.

[110] U. I. Atmaca, C. Maple, G. Epiphaniou *et al.*, "Challenges in threat modelling of new space systems: A teleoperation use-case," *Advances in Space Research*, vol. 70, no. 8, pp. 2208–2226, 2022.

[111] K. W. Ingols, "Design for security: Guidelines for efficient, secure small satellite computation," in *Proc. IEEE MTT-S Int. Microwave Symp. (IMS)*, 2017, pp. 226–228.

[112] G. Falco, A. Viswanathan, and A. Santangelo, "Cubesat security attack tree analysis," in *Proc. IEEE 8th Int. Conf. on Space Mission Challenges for Inform. Techn. (SMC-IT)*, 2021, pp. 68–76.

[113] J. Bouwmeester, A. Menicucci, and E. K. Gill, "Improving cubesat reliability: Subsystem redundancy or improved testing?" *Reliability Engineering & System Safety*, vol. 220, Art. no. 108288, 2022.

[114] 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, Art. no. 7286, 2022.

[115] T. M. Nguyen, "Future satellite system architectures and practical design issues: An overview," *Satellite Systems-Design, Modeling, Simulation and Analysis*, 2020.

[116] T. M. Braun, *Satellite Communications Payload and System*. John Wiley & Sons, Hoboken, NJ, 2012.

[117] A. Schalk, L. Brodnik, and D. Brown, "Analysis of vulnerabilities in satellite software bus network architecture," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 350–355.

[118] E. Kutlu, C. Gençtürk, R. Yiĝit, and F. N. Özcan, "Patch management of satellite flight software," in *Proc. 15th Turkish National Software Engineering Symposium (UYMS)*, 2021, pp. 1–5.

[119] P. Fortescue, G. Swinerd, and J. Stark, *Spacecraft Systems Engineering*. John Wiley & Sons, Hoboken, NJ, 2011.

[120] T. Kuwahara, K. Yoshida, Y. Sakamoto, Y. Tomioka, and K. Fukuda, "Satellite system integration based on space plug and play avionics," in *Proc. IEEE/SICE Int. Symp. on System Integr. (SII)*, 2011, pp. 896–901.

[121] Y. Nakamura, S. Fukuda, Y. Shibano, H. Ogawa, S.-i. Sakai, S. Shimizu, E. Soken, Y. Miyazawa, H. Toyota, A. Kukita *et al.*, "Exploration of energization and radiation in geospace (ERG): Challenges, development, and operation of satellite systems," *Earth, Planets and Space*, vol. 70, pp. 1–20, 2018.

[122] A. I. Perez-Neira, M. A. Vazquez, M. B. Shankar, S. Maleki, and S. Chatzinotas, "Signal processing for high-throughput satellites: Challenges in new interference-limited scenarios," *IEEE Signal Processing Magazine*, vol. 36, no. 4, pp. 112–131, 2019.

[123] I. del Portillo, B. Cameron, and E. Crawley, "Ground segment architectures for large LEO constellations with feeder links in EHF-bands," in *Proc. IEEE Aerospace Conf.*, 2018, pp. 1–14.

[124] B. Nejad, "The ground segment," in *Introduction to Satellite Ground Segment Systems Engineering: Principles and Operational Aspects*. Springer, Cham, 2023, pp. 57–68.

[125] B. Elbert, *The Satellite Communication Ground Segment and Earth Station Handbook*. Artech House, London, 2014.

[126] N. Ghani and S. Dixit, "TCP/IP enhancements for satellite networks," *IEEE Communications Magazine*, vol. 37, no. 7, pp. 64–72, 1999.

[127] G. Giambene and S. Kota, "Cross-layer protocol optimization for satellite communications networks: A survey," *Int. J. of Satellite Commun. and Netw.*, vol. 24, no. 5, pp. 323–341, 2006.

[128] G. Pan, J. Ye, Y. Tian, and M.-S. Alouini, "On HARQ schemes in satellite-terrestrial transmissions," *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 7998–8010, 2020.

[129] D. Perdices, G. Perna, M. Trevisan, D. Giordano, and M. Mellia, "When satellite is all you have: watching the internet from 550 ms," in *Proc. 22nd ACM Internet Measurement Conf.*, 2022, pp. 137–150.

[130] W. Ping, L. Guangxia, and D. Xin, "Design and performance analysis of accelerator to enhance TCP in satellite IP networks," in *Proc. IEEE Int. Conf. on Comp. Sci. and Netw. Techn.*, vol. 1, 2011, pp. 323–327.

[131] J. Zhu, S. Roy, and J. H. Kim, "Performance modelling of TCP enhancements in terrestrial–satellite hybrid networks," *IEEE/ACM Transactions on Networking*, vol. 14, no. 4, pp. 753–766, 2006.

[132] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, 2022.

[133] R. Scandariato, K. Wuyts, and W. Joosen, “A descriptive study of Microsoft’s threat modeling technique,” *Requirements Engineering*, vol. 20, pp. 163–180, 2015.

[134] A. Shostack, “Experiences threat modeling at Microsoft,” in *MODSEC@ MoDELS*, 2008, available from https://adam.shostack.org/modsec08, accessed Sept. 1, 2023.

[135] W. Xiong and R. Lagerström, “Threat modeling–a systematic literature review,” *Computers & Security*, vol. 84, pp. 53–69, 2019.

[136] X. Wu, Y. Du, T. Fan, J. Guo, J. Ren, R. Wu, and T. Zheng, “Threat analysis for space information network based on network security attributes: A review,” *Complex & Intelligent Systems*, vol. 9, no. 3, pp. 3429–3468, 2023.

[137] M. Usman, M. Qaraqe, M. R. Asghar, and I. Shafique Ansari, “Mitigating distributed denial of service attacks in satellite networks,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 6, Art. no. e3936, 2020.

[138] “Cyber considerations from the conflict in ukraine,” 2022. [Online]. Available: https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/03/cyber-considerations-from-the-conflict-in-ukraine.pdf

[139] “Strengthening cybersecurity of satcom network providers and customers,” 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

[140] T. Pfandzelter and D. Bermbach, “Failure is not an option: Considerations for software fault-tolerance in LEO satellite edge computing,” *arXiv preprint arXiv:2302.08952*, 2023.

[141] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, “Space odyssey: An experimental software security analysis of satellites,” in *Proc. IEEE Symp. on Sec. and Privacy*, 2023, pp. 1–19.

[142] H. Wu, F. Huang, P. Xiao, K. Fang, and J. Ou, “Secrecy satellite-terrestrial downlink transmissions against randomly located eavesdroppers,” *Trans. on Emerging Telecommun. Techn.*, vol. 34, no. 2, Art. no. e4686, 2023.

[143] M. Bradbury, C. Maple, H. Yuan, U. I. Atmaca, and S. Cannizzaro, “Identifying attack surfaces in the evolving space industry using reference architectures,” in *Proc. IEEE Aerosp. Conf.*, 2020, pp. 1–20.

[144] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, “DAG-based attack and defense modeling: Don’t miss the forest for the attack trees,” *Computer Science Review*, vol. 13, pp. 1–38, 2014.

[145] J. Pavur and I. Martinovic, “Building a launchpad for satellite cybersecurity research: Lessons from 60 years of spaceflight,” *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–17, 2022.

[146] S. Lohani and R. Joshi, “Satellite network security,” in *Proc. IEEE Int. Conf. on Emerging Trends in Communication, Control and Computing (ICONC3)*, 2020, pp. 1–5.

[147] A. A. Z. Hudaib, “Satellite network hacking & security analysis,” *International Journal of Computer Science and Security (IJCSS)*, vol. 10, no. 1, pp. 8–55, 2016.

[148] C. Konstantinou and M. Maniatakos, “Hardware-layer intelligence collection for smart grid embedded systems,” *Journal of Hardware and Systems Security*, vol. 3, pp. 132–146, 2019.

[149] B. Nussbaum and G. Berg, “Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure,” in *Space Infrastructures: From Risk to Resilience Governance*. IOS Press, Amsterdam, 2020, pp. 91–99.

[150] D. A. Galvan, B. Hemenway, W. Welser, and D. Baiocchi, *Satellite Anomalies: Benefits of a Centralized Anomaly Database and Methods for Securely Sharing Information Among Satellite Operators*. RAND Corp, Santa Monica, CA, 2014.

[151] K. Stoddart, “On cyberwar: Theorizing cyberwarfare through attacks on critical infrastructure—reality, potential, and debates,” in *Cyberwarfare: Threats to Critical Infrastructure*. Springer, 2022, pp. 53–146.

[152] C. Fleming, M. Reith, and W. Henry, “Securing commercial satellites for military operations: A cybersecurity supply chain framework,” in *Proc. Int. Conf. on Cyber Warfare and Security*, 2023, pp. 85–92.

[153] P. de Selding, “Eutelsat to field test new anti-jamming capability,” *Space News*, vol. 24, no. 4, 2013.

[154] N. Moustafa, I. A. Khan, M. Hassanin, D. Ormrod, D. Pi, I. Razzak, and J. Slay, “DFSat: Deep federated learning for identifying cyber threats in IoT-based satellite networks,” *IEEE Transactions on Industrial Informatics, in print*, 2024.

[155] J. Hayes, “Cyber security on satellites’ data: Evaluation of cryptography algorithms,” available from https://vsgc.odu.edu/wp-content/uploads/2022/07/Hayes.pdf, last accessed Apr. 30, 2023.

[156] N. Boschetti, N. Gordon, J. Sigholm, and G. Falco, “Commercial space risk framework assessing the satellite ground station security landscape for NATO in the arctic and high north,” in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 679–686.

[157] S. Lightman, T. Suloway, and J. Brule, “Satellite ground segment: Applying the cybersecurity framework to assure satellite command and control,” U.S. National Inst. of Standards and Techn. (NIST), Tech. Rep., 2022.

[158] J. Mangan, D. Murphy, R. Dunwoody, M. Doyle, A. Ulyanov, M. Hibbett, S. K. R. Akarapu, J. Erkal, G. Finneran, F. Marshall *et al.*, “Experiences in firmware development for a CubeSat instrument payload,” in *Proc. 4th Symp. on Space Educational Activities*, 2022, pp. 1–6.

[159] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, “Survey of publicly available reports on advanced persistent threat actors,” *Computers & Security*, vol. 72, pp. 26–59, 2018.

[160] B. Siregar, R. F. D. Purba, F. Fahmi *et al.*, “Intrusion prevention system against denial of service attacks using genetic algorithm,” in *Proc. IEEE Int. Conf. on Commun., Netw. and Satel. (Comnetsat)*, 2018, pp. 55–59.

[161] A. Di, S. Ruisheng, L. Lan, and L. Yueming, “On the large-scale traffic DDoS threat of space backbone network,” in *Proc. IEEE Int. Conf. on Intelligent Data and Security (IDS)*, 2019, pp. 192–194.

[162] W. Guo, J. Xu, Y. Pei, L. Yin, C. Jiang, and N. Ge, “A distributed collaborative entrance defense framework against DDoS attacks on satellite internet,” *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15 497–15 510, 2022.

[163] A. R. Shaaban, E. Abdelwanees, and M. Hussein, “Distributed denial of service attacks analysis, detection, and mitigation for the space control ground network: DDoS attacks analysis, detection and mitigation,” *Proc. of the Pakistan Academy of Sciences: A. Physical and Computational Sciences*, vol. 57, no. 2, pp. 97–108, 2020.

[164] Z. Tu, H. Zhou, K. Li, M. Li, and A. Tian, “An energy-efficient topology design and DDoS attacks mitigation for green software-defined satellite network,” *IEEE Access*, vol. 8, pp. 211 434–211 450, 2020.

[165] D. Agnew and J. McNair, “Detection of denial-of-service attacks in a software-defined LEO constellation network,” in *Governm. Microcircuit Appl. and Critical Techn. Conf. (GOMAC Tech)*, 2023, pp. 1–6.

[166] M. Jia, Y. Shu, Q. Guo, Z. Gao, and S. Xie, “DDoS attack detection method for space-based network based on SDN architecture,” *ZTE Communications*, vol. 18, no. 4, pp. 18–25, 2021.

[167] D. Vickramasingam and S. Bangar, “A link planning and DDoS attack detection in SDN based integrated space-terrestrial networks,” *Journal of Communications*, vol. 18, no. 4, pp. 267–273, 2023.

[168] M. Lehto, “Phenomena in the cyber world,” in *Cyber Security: Analytics, Technology and Automation*. Springer, Cham, 2015, pp. 3–29.

[169] Y. Liu, Y. Chen, Y. Jiao, H. Ma, and T. Wu, “A shared satellite ground station using user-oriented virtualization technology,” *IEEE Access*, vol. 8, pp. 63 923–63 934, 2020.

[170] A. Guptha, H. Murali, and T. Subbulakshmi, “A comparative analysis of security services in major cloud service providers,” in *Proc. 5th Int. Conf. on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 129–136.

[171] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *The Journal of Supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.

[172] C. Poole, R. Bettinger, and M. Reith, “Shifting satellite control paradigms: Operational cybersecurity in the age of megaconstellations,” *Air & Space Power Journal*, vol. 35, no. 3, pp. 46–56, 2021.

[173] G. Slocombe, “EW: Electronic warfare of increasing importance for the ADF,” *Asia-Pacific Defence Reporter (2002)*, vol. 47, no. 6, pp. 14–17, 2021.

[174] T. N. Nguyen, T. Van Chien, D.-H. Tran, V.-D. Phan, M. Voznak, S. Chatzinotas, Z. Ding, and H. V. Poor, “Security-reliability tradeoffs for satellite–terrestrial relay networks with a friendly jammer and imperfect csi,” *IEEE Trans. on Aerospace and Electronic Systems*, vol. 59, no. 5, pp. 7004–7019, 2023.

[175] J. Bardin, “Satellite cyber attack search and destroy,” in *Computer and Information Security Handbook (Third Edition)*. Elsevier, Boston, 2013, pp. 1173–1181.

[176] C. Weinbaum, S. Berner, and B. McClintock, *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain*. RAND Nat. Defense Research Inst. Santa Monica, CA, 2017.

[177] H. Fürtig, “Iran and the Arab spring: Between expectations and disillusion,” GIGA Working Papers, Tech. Rep., 2013.

[178] X.-C. Zheng and H.-M. Sun, “Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defined radio,” *Sensors and Materials*, vol. 32, no. 8, pp. 2729–2743, 2020.

[179] A. Costin, S. Khandker, H. Turtiainen, and T. Hämäläinen, “Cybersecurity of COSPAS-SARSAT and EPIRB: Threat and attacker models, exploits, future research,” *Proc. Network and Distributed*

System Security (NDSS) Symp., Workshop on Security of Space and Satellite Systems (SpaceSec), Feb. 2023, pp. 1–8.

[180] C. Van Camp and W. Peeters, "A world without satellite data as a result of a global cyber-attack," *Space Policy*, vol. 59, Art. no. 101458, 2022.

[181] D. Housen-Couriel, "Cybersecurity and anti-satellite capabilities (ASAT) new threats and new legal responses," *Journal of Law & Cyber Warfare*, vol. 4, no. 3, pp. 116–149, 2015.

[182] K. Zetter, "Russian spy gang hijacks satellite links to steal data," *Wired.com*, 2015.

[183] A. W. Green, A. B. Woszczynski, K. Dodson, and P. Easton, "Responding to cybersecurity challenges: Securing vulnerable US emergency alert systems," *Communications of the Association for Information Systems*, vol. 46, no. 1, pp. 187–208, Feb. 2020.

[184] A. S. Hamood and S. B. Sadkhan, "Cognitive radio network security status and challenges," in *Proc. IEEE Ann. Conf. on New Trends in Inform. & Commun. Techn. Appl. (NTICT)*, 2017, pp. 1–6.

[185] G. Zheng, Y. Yao, D. Wang, and J. Tian, "Study of an application of hybrid spread spectrum technology in satellite communication," in *Proc. Int. Conf. on Commun., Inform. System and Computer Eng. (CISCE)*, 2020, pp. 49–54.

[186] S. Kumar, P. Khanna, Pragya, and S. Tripathi, "Biometric assisted multi-modal encryption key for secured FHSS communication," in *Human-Centric Smart Computing*. Springer, Singapore, 2023, pp. 149–161.

[187] G. Andrea, "Cyber crime – from cyber space to outer space," Feb 2014. [Online]. Available: https://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/

[188] M. Torky, T. Gaber, E. Goda, V. Snasel, and A. E. Hassanien, "A blockchain protocol for authenticating space communications between satellites constellations," *Aerospace*, vol. 9, no. 9, Art. no. 495, 2022.

[189] R. Fratty, Y. Saar, R. Kumar, and S. Arnon, "Random routing algorithm for enhancing the cybersecurity of LEO satellite networks," *Electronics*, vol. 12, no. 3, Art. no. 518, 2023.

[190] G. Giuliari, T. Ciussani, A. Perrig, and A. Singla, "ICARUS: Attacking low earth orbit satellite networks," in *Proc. USENIX Ann. Techn. Conf.*, 2021, pp. 317–331.

[191] H. Li, D. Shi, W. Wang, D. Liao, T. R. Gadekallu, and K. Yu, "Secure routing for LEO satellite network survivability," *Computer Networks*, vol. 211, Art. no. 109011, 2022.

[192] Y. Yan, G. Han, and H. Xu, "A survey on secure routing protocols for satellite network," *J. Network and Computer Appl.*, vol. 145, Art. no. 102415, 2019.

[193] J. M. Rodriguez Bejarano, A. Yun, and B. De La Cuesta, "Security in IP satellite networks: COMSEC and TRANSEC integration aspects," in *Proc. 6th Adv. Satellite Multimedia Systems Conf. (ASMS) and 12th Signal Proc. for Space Commun. Workshop (SPSC)*, 2012, pp. 281–288.

[194] R. C. Benitez, "Cyber vulnerabilities in satellite communications networks," Ph.D. dissertation, Utica College, 2020.

[195] M. H. Abdulmonem, A. K. Ismail, and H. Mostafa, "Design and implementation of authenticated encryption co-processors for satellite hardware security," in *Proc. Int. Conf. on Microelectronics (ICM)*, 2021, pp. 40–44.

[196] M. A. V. Castro and F. Vieira, "DVB-S2 full cross-layer design for QoS provision," *IEEE Communications Magazine*, vol. 50, no. 1, pp. 128–135, 2012.

[197] A. Morello and U. Reimers, "DVB-S2, the second generation standard for satellite broadcasting and unicasting," *Int. J. Satellite Commun. and Netw.*, vol. 22, no. 3, pp. 249–268, 2004.

[198] A. Morello and V. Mignone, "DVB-S2: The second generation standard for satellite broad-band services," *Proceedings of the IEEE*, vol. 94, no. 1, pp. 210–227, 2006.

[199] M. Bowyer, L. Erup, and H. P. Lexow, "Security in dvb-rcs2," *Int. J. Satellite Commun. and Netw.*, vol. 31, no. 5, pp. 263–276, 2013.

[200] 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 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 277–284.

[201] Z. Zhao, N. Zhou, H. Zheng, P. Qin, and L. Yi, "Security enhancement for noise aggregation in DVB-S2 systems," in *Signal and Inform. Proc., Netw. and Comp.: Proc. 8th Int. Conf. on Signal and Inform. Proc., Netw. and Comp. (ICSINC)*. Springer, Singapore, 2022, pp. 326–334.

[202] H. Méric and L. Péricart, "Performance evaluation of a DVB-S2 system with a digital optical feeder link," *International Journal of Satellite Communications and Networking*, vol. 38, no. 6, pp. 463–479, 2020.

[203] Y. E. Sagduyu, T. Erpek, S. Ulukus, and A. Yener, "Is semantic communication secure? A tale of multi-domain adversarial attacks," *IEEE Communications Magazine*, vol. 61, no. 11, pp. 50–55, 2023.

[204] C. Baker and H. A. Kholidy, "Cyber security advantages of optical communications in SATCOM networks," Ph.D. dissertation, SUNY Polytechnic Institute, 2020.

[205] N. Lee and N. Lee, "Cyber warfare: Weapon of mass disruption," *Counterterrorism and Cybersecurity: Total Information Awareness*, pp. 201–248, 2015.

[206] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, vol. 18, pp. 129–163, 2019.

[207] N. Koroniotis, N. Moustafa, and J. Slay, "A new intelligent satellite deep learning network forensic framework for smart satellite networks," *Computers and Electrical Eng.*, vol. 99, Art. no. 107745, 2022.

[208] G. Falco, R. Thummala, and A. Kubadia, "Wannafly: An approach to satellite ransomware," in *Proc. IEEE 9th Int. Conf. on Space Mission Challenges for Information Techn. (SMC-IT)*, 2023, pp. 84–93.

[209] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (GDPR)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[210] B. Weeden and V. Samson, *Global counterspace capabilities: An open source assessment*. Secure World Foundation Washington, DC, Apr. 2018, available from https://swfound.org/counterspace/, Last accessed Sept. 1, 2023.

[211] H. S. Hudson, "Carrington events," *Annual Review of Astronomy and Astrophysics*, vol. 59, pp. 445–477, 2021.

[212] J. Drmola and T. Hubik, "Kessler syndrome: System dynamics model," *Space Policy*, vol. 44, pp. 29–39, 2018.

[213] M. Brown, S. Dey, G. Tuxworth, P. Bernus, and P. de Souza, "Dynamic verification of satellite systems using Ilities," *J. Space Safety Eng.*, vol. 9, no. 2, pp. 257–262, 2022.

[214] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, Art. no. 101701, 2020.

[215] M. B. Dunbar, I. Caballero, A. Román, and G. Navarro, "Remote sensing: Satellite and RPAS (remotely piloted aircraft system)," in *Marine Analytical Chemistry*. Springer, Cham, 2022, pp. 389–417.

[216] Y. Pang, D. Wang, D. Wang, L. Guan, C. Zhang, and M. Zhang, "A space-air-ground integrated network assisted maritime communication network based on mobile edge computing," in *Proc. IEEE World Congress on Services (SERVICES)*, 2020, pp. 269–274.

[217] W. A. Wheeler, N. Cohen, J. Betser, C. Meyers, W. Snavely, S. Chaki, M. Riley, and B. Runyon, "Cyber resilient flight software for spacecraft," in *Proc. AIAA SPACE and Astronautics Forum and Expo.*, 2017.

[218] L. Jones-Wilson, P. Cooley, A. Ralph, R. Largaespada, and D. Lee, "Europa clipper payload verification and validation: Test and analysis program design," in *Proc. IEEE Aerosp. Conf. (AERO)*, 2022, pp. 1–17.

[219] D. Kim, M. Gu, T.-H. Oh, E.-K. Kim, and H.-J. Yang, "Introduction of the advanced meteorological imager of Geo-Kompsat-2a: In-orbit tests and performance validation," *Remote Sensing*, vol. 13, no. 7, Art. no. 1303, 2021.

[220] K. Garane, M.-E. Koukouli, T. Verhoelst, C. Lerot, K.-P. Heue, V. Fioletov, D. Balis, A. Bais, A. Bazureau, A. Dehn *et al.*, "TROPOMI/S5P total ozone column data: Global ground-based validation and consistency with other satellite missions," *Atmospheric Measurement Techniques*, vol. 12, no. 10, pp. 5263–5287, 2019.

[221] Z. Zhima, B. Zhou, S. Zhao, Q. Wang, J. Huang, L. Zeng, J. Lei, Y. Chen, C. Li, D. Yang *et al.*, "Cross-calibration on the electromagnetic field detection payloads of the china seismo-electromagnetic satellite," *Science China Technological Sciences*, vol. 65, no. 6, pp. 1415–1426, 2022.

[222] D. Shangguan, L. Chen, and J. Ding, "A digital twin-based approach for the fault diagnosis and health monitoring of a complex satellite system," *Symmetry*, vol. 12, no. 8, Art. no. 1307, 2020.

[223] Z. Hóu, Q. Li, E. Foo, J. S. Dong, and P. de Souza, "A digital twin runtime verification framework for protecting satellites systems from cyber attacks," in *Proc. 26th Int. Conf. on Eng. of Complex Computer Systems (ICECCS)*, 2022, pp. 117–122.

[224] Z. Lai, Y. Deng, H. Li, Q. Wu, and Q. Zhang, "Space digital twin for secure satellite internet: Vulnerabilities, methodologies and future directions," *IEEE Network*, 2023.

[225] S. Mihai, M. Yaqoob, D. V. Hung, W. Davis, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, R. V. Prasad, H. Venkataraman, R. Trestian, and H. X. Nguyen, "Digital twins: A survey on enabling

technologies, challenges, trends and future prospects," *IEEE Commun. Surv. & Tut.*, vol. 24, no. 4, pp. 2255–2291, 2022.

[226] H. Xu, J. Wu, Q. Pan, X. Guan, and M. Guizani, "A survey on digital twin for industrial internet of things: Applications, technologies and tools," *IEEE COMST*, vol. 25, no. 4, pp. 2569–2598, 2023.

[227] Y. Zhou, R. Zhang, J. Liu, T. Huang, Q. Tang, and F. R. Yu, "A hierarchical digital twin network for satellite communication networks," *IEEE Commun. Mag.*, vol. 61, no. 11, pp. 104–110, 2023.

[228] B. Hayden, M. Sweeney, and B. Hale, "Securing software updates under receiver radio frequency geolocation risk," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 643–648.

[229] A. Zucherman, K. Jawork, A. Buchwald, A. Naikawadi, C. Robinson, E. Kumar, E. Kann, G. Orellana, M. Zakoworotny, O. Alon *et al.*, "Cislunar explorers: Lessons learned from the development of an interplanetary CubeSat," in *Proc. 34th AIAA/USU Conf. on Small Satellites*, 2020.

[230] A. Costin, H. Turtiainen, S. Khandker, and T. Hämäläinen, "Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications," *Proc. Workshop on Security of Space and Satellite Systems (SpaceSec), Network and Distributed System Security (NDSS) Symp.*, 2023, pp. 1–8.

[231] A. T. Azar, E. Shehab, A. M. Mattar, I. A. Hameed, and S. A. Elsaid, "Deep learning based hybrid intrusion detection systems to protect satellite networks," *Journal of Network and Systems Management*, vol. 31, no. 4, Art. no. 82, 2023.

[232] J. P. Thebarge, W. Henry, and G. Falco, "Developing scenarios supporting space-based IDS," in *Proc. ASCEND 2022*, 2022, pp. 4219:1–4219:12.

[233] R. Uddin and S. Kumar, "Federated learning based intrusion detection system for satellite communication," in *Proc. IEEE Cognitive Commun. for Aerospace Applications Workshop (CCAAW)*, 2023, pp. 1–6.

[234] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289–306, 2015.

[235] N.-T. Nguyen and C.-C. Chang, "A biometric-based authenticated key agreement protocol for user-to-user communications in mobile satellite networks," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1727–1758, 2019.

[236] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications," *Computer Communications*, vol. 147, pp. 85–97, 2019.

[237] J. Toivakka, "Network segmentation," 2018.

[238] J. Zhu and C. Wang, "Satellite networking intrusion detection system design based on deep learning method," in *Communications, Signal Processing, and Systems*. Springer Singapore, 2017, pp. 2295–2304.

[239] S. Salim, N. Moustafa, M. Hassanian, D. Ormod, and J. Slay, "Deep federated learning-based threat detection model for extreme satellite communications," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 3853–3867, 2024.

[240] S. J. H. Pirzada, A. Murtaza, L. Jianwei, and T. Xu, "Single event effects tolerant AES-CTR implementation for authentication of satellite communication," *Int. J. Computer and Commun. Eng.*, vol. 8, no. 4, pp. 178–183, 2019.

[241] S. Heron, "Advanced encryption standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, 2009.

[242] S. J. H. Pirzada, A. Murtaza, T. Xu, and L. Jianwei, "Architectural optimization of parallel authenticated encryption algorithm for satellite application," *IEEE Access*, vol. 8, pp. 48 543–48 556, 2020.

[243] S. Jeon, J. Kwak, and J. P. Choi, "Cross-layer encryption of CFB-AES-TURBO for advanced satellite data transmission security," *IEEE Trans. on Aerospace and Electronic Sys.*, vol. 58, no. 3, pp. 2192–2205, 2021.

[244] A. El Makhloufi, N. Chekroun, S. El Adib, and N. Raissouni, "Improved security approach based on AES algorithm for LST retrieval using satellite imagery in radiation-tolerant FPGAs," *Int. J. Embed. and Real-Time Commun. Sys.*, vol. 13, no. 1, pp. 1–17, 2022.

[245] M. Naim and A. Ali Pacha, "New chaotic satellite image encryption by using some or all the rounds of the AES algorithm," *Inform. Sec. Journ.: A Global Perspective*, vol. 32, no. 3, pp. 187–211, 2023.

[246] N. Aleisa, "A comparison of the 3DES and AES encryption standards," *Int. J. Security and Its Applications*, vol. 9, no. 7, pp. 241–246, 2015.

[247] Y. Ortakci and M. Y. Abdullah, "Performance analyses of AES and 3DES algorithms for encryption of satellite images," in *Innovations in Smart Cities Applications Volume 4: Proc. 5th Int. Conf. on Smart City Appl.* Springer, Cham, 2021, pp. 877–890.

[248] P. Preethi and G. Prakash, "Secure fusion of crypto-stegano based scheme for satellite image application," in *Proc. Asian Conf. on Innovation in Techn. (ASIANCON)*, 2021, pp. 1–6.

[249] M. Quan, Q. Jin, B. Ba, J. Zhang, and C. Jian, "Constellation encryption design based on chaotic sequence and the RSA algorithm," *Electronics*, vol. 11, no. 20, Art. no. 3346, 2022.

[250] J. Anderson, S. Lo, A. Neish, and T. Walter, "Authentication of satellite-based augmentation systems with over-the-air rekeying schemes," *NAVIGATION: Journal of the Institute of Navigation*, vol. 70, no. 3, pp. 1–31, 2023.

[251] J. Guo, Y. Du, Y. Zhang, and M. Li, "A provably secure ECC-based access and handover authentication protocol for space information networks," *J. Network and Computer Appl.*, vol. 193, Art. no. 103183, 2021.

[252] J. Guo, Y. Du, D. Zhang, and R. Wu, "PSEEMV: Provably secure and efficient emergency message verification scheme based on ECC and CRT for space information network," *J. Information Security and Appl.*, vol. 73, Art. no. 103437, 2023.

[253] C. Poomagal and G. Sathish Kumar, "ECC based lightweight secure message conveyance protocol for satellite communication in internet of vehicles (IoV)," *Wireless Personal Communications*, vol. 113, pp. 1359–1377, 2020.

[254] R. Hirokawa, S. Fujita, and N. Hayase, "The first satellite-based open PPP-RTK service: Operational experiences and improvements," in *Proc. 36th Int. Techn. Meeting of the Satellite Div. of The Inst. of Navigation*, 2023, pp. 469–482.

[255] M. Juliato and C. Gebotys, "SEU-resistant SHA-256 design for security in satellites," in *Proc. IEEE 10th Int. Workshop on Sig. Proc. for Space Commun.*, 2008, pp. 1–7.

[256] M. Juliato, C. Gebotys, and R. Elbaz, "Efficient fault tolerant SHA-2 hash functions for space applications," in *Proc. IEEE Aerospace Conf.*, 2009, pp. 1–16.

[257] I. Altaf, M. Arslan Akram, K. Mahmood, S. Kumari, H. Xiong, and M. Khurram Khan, "A novel authentication and key-agreement scheme for satellite communication network," *Trans. on Emerging Telecommun. Techn.*, vol. 32, no. 7, Art. no. e3894, 2021.

[258] Z. Ruan, X. Yang, H. Luo, X. Yang, Y. Miao, X. Huang, and X. Yi, "A robust and secure data access scheme for satellite-assisted Internet of Things with content adaptive addressing," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 13393–13410, 2024.

[259] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, "Dynamic role-based access control policy for smart grid applications: An offline deep reinforcement learning approach," *IEEE Transactions on Human-Machine Systems*, vol. 52, no. 4, pp. 761–773, 2022.

[260] Z. Wu, R. Liu, and H. Cao, "ECDSA-based message authentication scheme for BeiDou-II navigation satellite system," *IEEE Trans. on Aerospace and Electr. Sys.*, vol. 55, no. 4, pp. 1666–1682, 2018.

[261] A.-D. Tudosi, D. G. Balan, and A. D. Potorac, "Secure network architecture based on distributed firewalls," in *Proc. Int. Conf. on Development and Application Systems (DAS)*, 2022, pp. 85–90.

[262] A. Mehdizadeha, K. Suinggia, M. Mohammadpoorb, and H. Haruna, "Virtual local area network (VLAN): Segmentation and security," in *Proc. Third Int. Conf. on Computing Technology and Information Management (ICCTIM)*, 2017, pp. 78–89.

[263] I. Ashraf, M. Narra, M. Umer, R. Majeed, S. Sadiq, F. Javaid, and N. Rasool, "A deep learning-based smart framework for cyber-physical and satellite system security threats detection," *Electronics*, vol. 11, no. 4, Art. no. 667, 2022.

[264] J. Ye, H. Gharavi, and B. Hu, "Fast beam discovery and adaptive transmission under frequency selective attenuations in sub-terahertz bands," *IEEE Trans. Signal Proc.*, vol. 71, pp. 727–740, 2023.

[265] B. Gao, Z. Fan, X. Liu, L. Zhang, and X. Ouyang, "OFDM covert communication system based on the QC-LDPC and symbol spread spectrum," in *Proc. Cross Strait Radio Science & Wireless Techn. Conf. (CSRSWTC)*, 2020, pp. 1–3.

[266] A. Bhattacharyya, S. M. Nambiar, R. Ojha, A. Gyaneshwar, U. Chadha, and K. Srinivasan, "Machine learning and deep learning powered satellite communications: Enabling technologies, applications, open challenges, and future research directions," *Int. J. Satellite Commun. and Netw.*, vol. 41, no. 6, pp. 539–588, Nov./Dec. 2023.

[267] A. Shaikh and P. Gupta, "Advanced signature-based intrusion detection system," in *Intelligent Communication Technologies and Virtual Mobile Networks*. Springer, Singapore, 2023, pp. 305–321.

[268] R. Samrin and D. Vasumathi, "Review on anomaly-based network intrusion detection system," in *Proc. Int. Conf. on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, 2017, pp. 141–147.

[269] M. A. Obied, F. F. Ghaleb, A. E. Hassanien, A. M. Abdelfattah, and W. Zakaria, "Deep clustering-based anomaly detection and health monitoring for satellite telemetry," *Big Data and Cognitive Computing*, vol. 7, no. 1, Art. no. 39, 2023.

[270] C. She, Y. Ma, L. Jia, L. Fei, and B. Kou, "Intrusion-detection model integrating anomaly with misuse for space information network," *J. Commun. and Information Netw.*, vol. 1, no. 3, pp. 90–96, 2016.

[271] 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, Art. no. 22261, 2021.

[272] K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, "Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," *IEEE Access*, vol. 8, pp. 214 852–214 865, 2020.

[273] U. Uhongora, R. Mulinde, Y. W. Law, and J. Slay, "Deep-learning-based intrusion detection for software-defined networking space systems," in *Proc. European Conf. on Cyber Warfare and Security*, vol. 22, no. 1, 2023, pp. 639–647.

[274] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, Art. no. 4759, 2021.

[275] Z. Wen-bo, S. Peigen, L. Zhi-guo, and X. Haifeng, "An intrusion detection model for satellite network," in *Proc. 2nd IEEE Int. Conf. on Inform. Management and Eng.*, 2010, pp. 167–170.

[276] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, 2020.

[277] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217 463–217 472, 2020.

[278] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, "Federated wireless network intrusion detection," in *Proc. IEEE International Conference on Big Data (Big Data)*, 2019, pp. 6004–6006.

[279] R. Kumar and S. Arnon, "Enhancing cybersecurity of satellites at Sub-THz bands," in *Proc. 6th Int. Symp. Cyber Security, Cryptology, and Machine Learning (CSCML)*. Springer, Cham, 2022, pp. 356–365.

[280] M. G. Schraml, A. Knopp, and K.-U. Storek, "Multi-user MIMO satellite communications with secrecy constraints," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2019, pp. 17–22.

[281] M. G. Schraml and A. Knopp, "Precoding for security gap physical layer security in multiuser MIMO satellite systems," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 612–617.

[282] K. S. J. Yap, "A network intrusion detection system using decision tree machine learning on an ISTN architecture," Naval Postgraduate School Monterey, CA, Tech. Rep., 2022.

[283] T. Rupa Devi and S. Badugu, "A review on network intrusion detection system using machine learning," *Advances in Decision Sciences, Image Processing, Security and Computer Vision*, pp. 598–607, 2020.

[284] R. Kumar and S. Arnon, "Leveraging atmospheric effects with LSTM for ensuring cybersecurity of satellite links," *TechRxiv*, 2022.

[285] A. Georgescu, A. V. Gheorghe, M.-I. Piso, and P. F. Katina, "Critical space infrastructure interdependencies," in *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer, Cham, 2019, pp. 79–139.

[286] M. Chen, S. Guo, X. Huang, L. Su, and H. Du, "Research on secure access in converged satellite and terrestrial networks," in *Proc. IEEE 31st Int. Conf. on Network Protocols (ICNP)*, 2023, pp. 1–6.

[287] J. Zhao, S. Li, X. Xu, H. Yan, and Z. Zhang, "Adaptive resource allocation of secured access to intelligent surface enhanced satellite-terrestrial networks with two directional traffics," *AEU-Int. J. of Electr. and Commun.*, vol. 170, Art. no. 154746, 2023.

[288] O. Challa, G. Bhat, and J. McNair, "CubeSec and GndSec: A lightweight security solution for CubeSat communications," in *Proc. 26th Ann. AIAA/USU Conf. on Small Satellites*, 2012, pp. 1–8.

[289] H. Schaub, L. E. Jasper, P. V. Anderson, and D. S. McKnight, "Cost and risk assessment for spacecraft operation decisions caused by the space debris environment," *Acta Astronautica*, vol. 113, pp. 66–79, 2015.

[290] G. Hills, J. Baldasare, W. Henry, and W. Connell, "A customized approach to cybersecurity education for space professionals," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 160–165.

[291] P.K. Martin, "*NASA Cybersecurity: An Examination of the Agency's Information Security*, U.S. Government Publishing Office, House Hearing, 112 Congress, Serial No. 112-64, Feb. 2012.

[292] R. Bagnara, "MISRA C, for security's sake!" *CoRR*, vol. abs/1705.03517, 2017. [Online]. Available: http://arxiv.org/abs/1705.03517

[293] U.S. National Institute of Standards and Technology (NIST), "Security and privacy controls for federal information systems and organizations, nist special publication 800-53, revision 5," Sep. 2020.

[294] S. Jeong, S. Lee, and J. Kim, "Fault management system using penalty method and data buffer for communication satellite," in *Proc. 24th AIAA Int. Commun. Satellite Sys. Conf.*, 2006, Paper no. 5332.

[295] J. G. Tront, J. R. Armstrong, and J. V. Oak, "Software techniques for detecting single-event upsets in satellite computers," *IEEE Transactions on Nuclear Science*, vol. 32, no. 6, pp. 4225–4228, 1985.

[296] M. Tipaldi and B. Bruenjes, "Survey on fault detection, isolation, and recovery strategies in the space domain," *J. Aerospace Information Sys.*, vol. 12, no. 2, pp. 235–256, 2015.

[297] Z. Zheng, J. Guo, and E. Gill, "Onboard autonomous mission replanning for multi-satellite system," *Acta Astronautica*, vol. 145, pp. 28–43, 2018.

[298] H.W. Zaglauer, et al., "Integrated satellite access to 5G/6G systems–An overview of the 5G space infrastructure study," in *Proc. IET 39th Int. Commun. Satellite Sys. Conf. (ICSSC)*, 2023, pp. 76–83.

[299] H. Jahankhani, S. Kendzierskyj, and O. Hussien, "Approaches and methods for regulation of security risks in 5G and 6G," in *Wireless Networks: Cyber Security Threats and Countermeasures*. Springer, Cham, 2023, pp. 43–70.

[300] X. Cui and Y. Gao, "Research on security system of satellite-ground integrated virtual private network in 6G," in *Proc. IEEE 2nd Int. Conf. on Computing, Communication, Perception and Quantum Technology (CCPQT)*, 2023, pp. 202–206.

[301] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi, C. Wang, X. Shao, M. Reisslein, and H. ElBakoury, "Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research," *IEEE COMST*, vol. 21, no. 1, pp. 88–145, 2019.

[302] D. Rico and P. Merino, "A survey of end-to-end solutions for reliable low-latency communications in 5G networks," *IEEE Access*, vol. 8, pp. 192 808–192 834, 2020.

[303] Z. Xiang, F. Gabriel, E. Urbano, G. T. Nguyen, M. Reisslein, and F. H. Fitzek, "Reducing latency in virtual machines: Enabling tactile internet for human-machine co-working," *IEEE JSAC*, vol. 37, no. 5, pp. 1098–1116, 2019.

[304] S.-C. Lin, C.-H. Lin, L. C. Chu, and S.-Y. Lien, "Enabling resilient access equality for 6G LEO satellite swarm networks," *IEEE Internet of Things Mag.*, vol. 6, no. 3, pp. 38–43, 2023.

[305] 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.

[306] G. Masini, P. Reininger, M. El Jaafari, A. Vesely, N. Chuberre, B. Baudry, and J.-M. Houssin, "5G meets satellite: Non-terrestrial network architecture and 3GPP," *Int. J. of Satellite Commun. and Netw.*, vol. 41, no. 3, pp. 249–261, 2023.

[307] 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. Standards Mag.*, vol. 5, no. 4, pp. 147–153, 2021.

[308] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165 178–165 200, 2020.

[309] A. Sattarzadeh, Y. Liu, A. Mohamed, R. Song, P. Xiao, Z. Song, H. Zhang, R. Tafazolli, and C. Niu, "Satellite-based non-terrestrial networks in 5G: Insights and challenges," *IEEE Access*, vol. 10, pp. 11 274–11 283, 2022.

[310] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5g advances and the road toward 6G," *IEEE COMST*, vol. 24, no. 2, pp. 1117–1174, 2022.

[311] F. Völk, T. Schlichter, F. Kaltenberger, T. Heyn, G. Casati, R. T. Schwarz, and A. Knopp, "Field trial of a 5G non-terrestrial network using OpenAirInterface," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 243–250, 2022.

[312] Z. Bai, et al., "On-orbit demonstration of inter-satellite free-space optical stable communication enabled by integrated optical amplification of HPA and LNA," *Appl. Opt.*, vol. 62, no. 23, pp. G18–G25, 2023.

[313] D.R Kolev, et al., "Latest developments in the field of optical communications for small satellites and beyond," *Journal of Lightwave Technology*, vol. 41, no. 12, pp. 3750–3757, 2023.

[314] J. G. Olmedo and V. P. G. Jiménez, "Visibility framework and performance analysis for free space optical communications in satellite links," *IEEE Access*, vol. 11, pp. 68 897–68 911, 2023.

[315] I. P. Vieira, T. C. Pita, and D. A. A. Mello, "Modulation and signal processing for LEO-LEO optical inter-satellite links," *IEEE Access*, vol. 11, pp. 63 598–63 611, 2023.

[316] G. Kim and H. Kim, "Link reliability of satellite-to-ground free-space optical communication systems in South Korea," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2022, pp. 618–622.

[317] E. Erdogan, O. B. Yahia, G. K. Kurt, and H. Yanikomeroglu, "Optical HAPS eavesdropping in vertical heterogeneous networks," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 208–216, 2023.

[318] Z. Pan and I. B. Djordjevic, "Secret key distillation over satellite-to-satellite free-space optics channel with a limited-sized aperture eavesdropper in the same plane of the legitimate receiver," *Optics Express*, vol. 28, no. 25, pp. 37 129–37 148, 2020.

[319] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "Optical satellite eavesdropping," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 10 126–10 131, 2022.

[320] Y. Tian, G. Pan, H. ElSawy, and M.-S. Alouini, "Satellite-aerial communications with multi-aircraft interference," *IEEE Trans. on Wireless Communications*, vol. 22, no. 10, pp. 7008–7024, 2023.

[321] J. Liu, Z. Yang, Z. Wu, Z. Yin, X. Jiang, and Y. Fu, "Control code multiple encryption algorithm on satellite-to-ground communication," *Mob. Netw. and Appl.*, vol. 24, no. 6, pp. 1955–1974, 2019.

[322] Y. Zhang, et al., "A survey of secure communications for satellite internet based on cryptography and physical layer security," *IET Information Security*, vol. 2023, Art. no. 5604802, 2023.

[323] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G.-H. Tu, "The security in optical wireless communication: A survey," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 329:1–329:36, Jul. 2023.

[324] E. Illi, F. El Bouanani, F. Ayoub, and M.-S. Alouini, "A PHY layer security analysis of a hybrid high throughput satellite with an optical feeder link," *IEEE Open Journal of the Commun. Soc.*, vol. 1, pp. 713–731, 2020.

[325] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surv. & Tut.*, vol. 19, no. 1, pp. 57–96, 2016.

[326] Y. Xiao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure communication in non-geostationary orbit satellite systems: A physical layer security perspective," *IEEE Access*, vol. 7, pp. 3371–3382, 2018.

[327] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Höyhtyä, "Security of satellite-terrestrial communications: Challenges and potential solutions," *IEEE Access*, vol. 10, pp. 96 038–96 052, 2022.

[328] A. Iqbal, M.-L. Tham, Y. J. Wong, A. Al-Habashna, G. Wainer, Y. X. Zhu, and T. Dagiuklas, "Empowering non-terrestrial networks with artificial intelligence: A survey," *IEEE Access*, vol. 11, pp. 100 986–101 006, 2023.

[329] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010–1038, 2020.

[330] B. K. Tripathy, S. K. Jena, P. Bera, and S. Das, "An adaptive secure and efficient routing protocol for mobile ad hoc networks," *Wireless Personal Communications*, vol. 114, pp. 1339–1370, 2020.

[331] M.-E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, "Cyber risk management for critical infrastructure: a risk analysis model and three case studies," *Risk Analysis*, vol. 38, no. 2, pp. 226–241, 2018.

[332] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[333] Q. T. Ngo, K. T. Phan, A. Mahmood, and W. Xiang, "Physical layer security in IRS-assisted cache-enabled satellite communication networks," *IEEE Trans. on Green Communications and Networking*, vol. 7, no. 4, pp. 1920–1931, 2023.

[334] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[335] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Let.*, vol. 17, no. 7, pp. 1483–1486, 2013.

[336] R. Dong, B. Wang, and K. Cao, "Deep learning driven 3D robust beamforming for secure communication of UAV systems," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1643–1647, 2021.

[337] N. Abdelsalam, S. Al-Kuwari, and A. Erbad, "Physical layer security in satellite communication: State-of-the-art and open problems," *arXiv preprint arXiv:2301.03672*, 2023.

[338] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, vol. 36, no. 3, pp. 98–104, 2022.

[339] R. Singh, I. Ahmad, and J. Huusko, "The role of physical layer security in satellite-based networks," *Proc. IEEE European Conf. on Networks and Commun. & 6G Summit (EuCNC/6G Summit*, 2023, pp. 36–41.

[340] C. Fu, C. Wang, and D. Cai, "High dimensional similarity search with satellite system graph: Efficiency, scalability, and unindexed query compatibility," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 8, pp. 4139–4150, 2021.

[341] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, "Quantum key distribution over double-layer quantum satellite networks," *IEEE Access*, vol. 8, pp. 16 087–16 098, 2020.

[342] O. Popescu, "Power budgets for CubeSat radios to support ground communications and inter-satellite links," *IEEE Access*, vol. 5, pp. 12 618–12 625, 2017.

[343] O. T. H. Alzubaidi, M. N. Hindia, K. Dimyati, K. A. Noordin, A. N. A. Wahab, F. Qamar, and R. Hassan, "Interference challenges and management in B5G network design: A comprehensive review," *Electronics*, vol. 11, no. 18, Art. no. 2842, 2022.

[344] B. Peccerillo, M. Mannino, A. Mondelli, and S. Bartolini, "A survey on hardware accelerators: Taxonomy, trends, challenges, and perspectives," *J. Sys. Arch.*, vol. 129, Art. no. 102561, Aug. 2022.

[345] P. Shantharama, A. S. Thyagaturu, and M. Reisslein, "Hardware-accelerated platforms and infrastructures for network functions: A survey of enabling technologies and research studies," *IEEE Access*, vol. 8, pp. 132 021–132 085, 2020.

[346] B. Barbour, R. Gibbons, S. Kenyon, J. McClure, D. Ridge, and J. Black, "Network testbed for small satellites (NeTSat)-distributed space adaptive communications and security for multi-constellation networks," in *Proc. AIAA SCITECH 2023 Forum*, Jan. 2023, Paper no. 1502.

[347] J. Huwyler, J. Pavur, G. Tresoldi, and M. Strohmeier, "QPEP in the real world: A testbed for secure satellite communication performance," in *Proc. Workshop Sec. of Space and Satel. Sys.*, Feb. 2023, pp. 1–9.

[348] I. Marboe, *Small Satellites: Regulatory Challenges and Chances*. Brill, Netherlands, 2016.

[349] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2019.

[350] R. Picchi, F. Chiti, R. Fantacci, and L. Pierucci, "Towards quantum satellite internetworking: A software-defined networking perspective," *IEEE Access*, vol. 8, pp. 210 370–210 381, 2020.

[351] 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 Communication*, vol. 2, no. 4, pp. 182–217, 2021.

[352] D. Zhu, H. Zhu, Z. Wang, and Y. Zhang, "Three-level quantum satellite communication framework and its applications," *Int. J. Satellite Communications and Networking*, vol. 39, no. 5, pp. 473–485, 2021.

[353] J. Chen, "Review on quantum communication and quantum computation," in *Journal of Physics: Conference Series*, vol. 1865, no. 2. IOP Publishing, 2021, Art no. 022008.

[354] I. B. Djordjevic, "On global quantum communication networking," *Entropy*, vol. 22, no. 8, Art. no. 831, 2020.

[355] S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Physical Review Research*, vol. 3, no. 2, Art. no. 023130, 2021.

[356] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Communications*, vol. 16, no. 10, pp. 1–36, 2019.

[357] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[358] W. Weaver, "Recent contributions to the mathematical theory of communication," *ETC: A Review of General Semantics*, vol. 10, no. 4, pp. 261–281, Summer 1953.

[359] M. Chafii, L. Bariah, S. Muhaidat, and M. Debbah, "Twelve scientific challenges for 6G: Rethinking the foundations of communications theory," *IEEE COMST*, vol. 25, no. 2, pp. 868–904, 2023.

[360] K. Lu, Q. Zhou, R. Li, Z. Zhao, X. Chen, J. Wu, and H. Zhang, "Rethinking modern communication from semantic coding to semantic communication," *IEEE Wireless Communications*, vol. 30, no. 1, pp. 158–164, 2023.

[361] S. Rezwan, H. Wu, J. Cabrera, G. Nguyen, M. Reisslein, and F. Fitzek, "cXR+ voxel-based semantic compression for networked immersion," *IEEE Access*, vol. 11, pp. 52 763–52 777, 2023.

[362] E. Uysal, O. Kaya, A. Ephremides, J. Gross, M. Codreanu, P. Popovski, M. Assaad, G. Liva, A. Munari, B. Soret *et al.*, "Semantic communications in networked systems: A data significance perspective," *IEEE Network*, vol. 36, no. 4, pp. 233–240, 2022.

[363] W. Yang, H. Du, Z. Q. Liew, W. Y. B. Lim, Z. Xiong, D. Niyato, X. Chi, X. Shen, and C. Miao, "Semantic communications for future internet: Fundamentals, applications, and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 25, no. 1, pp. 213–250, 2023.

[364] Y. Lin, H. Du, D. Niyato, J. Nie, J. Zhang, Y. Cheng, and Z. Yang, "Blockchain-aided secure semantic communication for AI-generated content in metaverse," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 72–83, 2023.

[365] X. Luo, Z. Chen, M. Tao, and F. Yang, "Encrypted semantic communication using adversarial training for privacy preserving," *IEEE Communications Letters*, vol. 27, no. 6, pp. 1486–1490, 2023.

[366] Z. Yang, M. Chen, G. Li, Y. Yang, and Z. Zhang, "Secure semantic communications: Fundamentals and challenges," *arXiv preprint arXiv:2301.01421*, 2023.

[367] S. Derebeyoğlu, C. Deppe, and R. Ferrara, "Performance analysis of identification codes," *Entropy*, vol. 22, no. 10, Art. no. 1067, 2020.

[368] T. S. Han and S. Verdú, "New results in the theory of identification via channels," *IEEE Trans. Inform. Th.*, vol. 38, no. 1, pp. 14–25, 1992.

[369] C. von Lengerke, A. Hefele, J. Cabrera, M. Reisslein, and F. Fitzek, "Beyond the bound: A new performance perspective for identification via channels," *IEEE JSAC*, vol. 41, no. 8, pp. 2687–2706, 2023.

[370] C. V. Lengerke, A. Hefele, J. A. Cabrera, O. Kosut, M. Reisslein, and F. H. P. Fitzek, "Identification codes: A topical review with design guidelines for practical systems," *IEEE Access*, vol. 11, pp. 14 961–14 982, 2023.

[371] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, and J. d. J. Lozoya-Santos, "Digital twin technology challenges and applications: A comprehensive review," *Remote Sensing*, vol. 14, no. 6, Art. no. 1335, 2022.

[372] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong, "Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities," *IEEE COMST*, vol. 24, no. 4, pp. 2230–2254, 2022.

[373] F. Tao, B. Xiao, Q. Qi, J. Cheng, and P. Ji, "Digital twin modeling," *Journal of Manufacturing Systems*, vol. 64, pp. 372–389, 2022.

[374] S. Baur, C. Deppe, and H. Boche, "Secure storage for identification; random resources and privacy leakage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2013–2027, 2019.

[375] H. Boche, C. Deppe, and A. Winter, "Secure and robust identification via classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 65, no. 10, pp. 6734–6749, 2019.

[376] H. Fan, J. Long, L. Liu, and Z. Yang, "Dynamic digital twin and online scheduling for contact window resources in satellite network," *IEEE Trans. on Industr. Inform.*, vol. 19, no. 5, pp. 7217–7227, 2023.

[377] L. Zhao, C. Wang, K. Zhao, D. Tarchi, S. Wan, and N. Kumar, "INTERLINK: A digital twin-assisted storage strategy for satellite-terrestrial networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 3746–3759, 2022.

[378] N. Cai and T. Chan, "Theory of secure network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[379] D. E. Lucani, M. V. Pedersen, D. Ruano, C. W. Sørensen, F. H. Fitzek, J. Heide, O. Geil, V. Nguyen, and M. Reisslein, "Fulcrum: Flexible network coding for heterogeneous devices," *IEEE Access*, vol. 6, pp. 77 890–77 910, 2018.

[380] R. Wu, J. Ma, Z. Tang, X. Li, and K.-K. R. Choo, "A generic secure transmission scheme based on random linear network coding," *IEEE/ACM Trans. on Networking*, vol. 30, no. 2, pp. 855–866, 2021.

[381] S. Wunderlich, J. A. Cabrera, F. H. Fitzek, and M. Reisslein, "Network coding in heterogeneous multicore IoT nodes with DAG scheduling of parallel matrix block operations," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 917–933, 2017.

[382] J. Cloud and M. Médard, "Network coding over SATCOM: Lessons learned," in *Proc. 7th Int. Conf. on Wireless and Satellite Systems (WiSATS)*. Springer, Cham, 2015, pp. 272–285.

[383] U. Speidel, L. Qian, E. Cocker, M. Médard, P. Vingelmann, and J. Heide, "Topologies and coding considerations for the provision of network-coded services via shared satellite channels," *Intl. J. on Advances in Telecommunications*, vol. 10, no. 3&4, pp. 175–185, 2017.

[384] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 9, pp. 1862–1874, 2015.

[385] G. Peralta, R. G. Cid-Fuentes, J. Bilbao, and P. M. Crespo, "Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges," *Electronics*, vol. 8, no. 8, Art. no. 827, 2019.

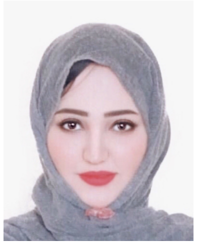
[386] H. Tang, Q. T. Sun, X. Yang, and K. Long, "A network coding and DES based dynamic encryption scheme for moving target defense," *IEEE Access*, vol. 6, pp. 26 059–26 068, 2018.

[387] E. Tasdemir, M. Tömösközi, J. A. Cabrera, F. Gabriel, D. You, F. H. Fitzek, and M. Reisslein, "SpaRec: Sparse systematic RLNC recoding in multi-hop networks," *IEEE Access*, vol. 9, pp. 168 567–168 586, 2021.

[388] E. Tasdemir, V. Nguyen, G. T. Nguyen, F. H. Fitzek, and M. Reisslein, "FSW: Fulcrum sliding window coding for low-latency communication," *IEEE Access*, vol. 10, pp. 54 276–54 290, 2022.

[389] A. Tassi, R. J. Piechocki, and A. Nix, "On intercept probability minimization under sparse random linear network coding," *IEEE Trans. on Vehicular Technology*, vol. 68, no. 6, pp. 6137–6141, 2019.

[390] A. Zarei, P. Pahlevani, and D. E. Lucani, "An analytical model for sparse network codes: Field size considerations," *IEEE Communications Letters*, vol. 24, no. 4, pp. 729–733, 2020.



Sara Salim is currently a research associate at the Australian Defense Force, Canberra, affiliated with the University of New South Wales (UNSW). She completed her PhD in cybersecurity from the School of Engineering and Information Technology (SEIT) at UNSW, Canberra, in 2023. Before that, she obtained her Bachelor's degree in Computer Science from the Faculty of Computer and Information at Zagazig University, Egypt, and her Master's degree in Optimization and Operations Research Applications from the Faculty of Computer and Information at Menoufia University, Egypt. Her research focuses on the intersection of cybersecurity, artificial intelligence-based learning, and the security of heterogeneous devices and future networks. She is particularly interested in social networks, the Internet of Things, and satellite communications.

Nour Moustafa is an ARC DECRA Fellow & Leader of Intelligent Security Hub, University of New South Wales (UNSW)'s UNSW Canberra, Australia. He was a Post-doctoral Fellow at UNSW Canberra from June 2017 till December 2018. He received his PhD degree in the field of Cyber Security from UNSW Canberra in 2017. He obtained his Bachelor's and Master's degrees in Computer Science in 2009 and 2014, respectively, from the Faculty of Computer and Information, Helwan University, Egypt. His areas of interest include Cyber Security, in particular, Network Security, IoT security, intrusion detection systems, statistics, Deep learning and machine learning techniques. He has several research grants totaling over AUD 1.2 Million. He has been awarded the 2020 prestigious Australian Spitfire Memorial Defence Fellowship award. He is also a Senior IEEE Member, ACM Distinguished Speaker. He has served his academic community, as the guest associate editor of IEEE Transactions journals, including IEEE Transactions on Industrial Informatics, IEEE IoT Journal, as well as the journals IEEE Access, Future Internet and Information Security Journal: A Global Perspective. He has also served over seven conferences in leadership roles, involving vice-chair, session chair, Technical Program Committee (TPC) member and proceedings chair, including 2020–2022 IEEE TrustCom and 2020 33rd Australasian Joint Conference on Artificial Intelligence.

Martin Reisslein (S'96-M'98-SM'03-F'14) received the Ph.D. in systems engineering from the University of Pennsylvania, Philadelphia, PA, USA in 1998. He is currently a Professor with the School of Electrical, Computer, and Energy Engineering, Arizona State University (ASU), Tempe, AZ, USA, and Program Chair of the Computer Engineering (CEN) program at ASU. He is currently an Associate Editor for *IEEE Access* and *IEEE Transactions on Network and Service Management*. He currently serves Area Editor for Optical Communications for the *IEEE Communications Surveys and Tutorials* and as Co-Editor-in-Chief of *Optical Switching and Networking*.