international journal of critical infrastructure protection 47 (2024) 100724

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions

Shah Khalid Khan [a,b,*], Nirajan Shiwakoti [b], Abebe Diro [c], Alemayehu Molla [c], Iqbal Gondal [b], Matthew Warren [a,d]

[a] Centre for Cyber Security Research and Innovation, RMIT University Melbourne, Australia
[b] School of Engineering, RMIT University Melbourne, Australia
[c] Department of Information Systems and Business Analytics, RMIT University, Melbroune, Australia
[d] University of Johannesburg, South Africa

ARTICLE INFO

Keywords:
Security
Outer space, Low earth orbit, Commercial-off-the-shelf

ABSTRACT

Space Cybersecurity (SC) is becoming critical due to the essential role of space in global critical infrastructure – enabling communication, safe air travel, maritime trade, weather monitoring, environmental surveillance, financial services, and defence systems. Simultaneously, involving diverse stakeholders in space operations further amplifies this criticality. Similarly, previous research has identified isolated vulnerabilities in SC and proposed individual solutions to mitigate them. While such studies have provided useful insights, they do not offer a comprehensive analysis of space cyber-attack vectors and a critical evaluation of the effectiveness of mitigation strategies. This study addresses this problem by holistically examining the scope of potential space cyber-attack vectors, encompassing the ground, space, user, cloud, communication channels, and supply chain segments. Furthermore, the study evaluates the effectiveness of legacy security controls and frameworks and outlines SC-vector-aligned counterstrategies and mitigation techniques to tackle the unique SC threats. Based on the analysis, the study proposes future research directions to develop and test advanced technological solutions and regulatory and operational frameworks to establish international standards policies and foster stakeholder collaboration. The study contributes a multi-disciplinary foundation and roadmap that researchers, technology developers, and decision-makers can draw on in shaping a robust and sustainable SC framework.

1. Introduction

Digital transformation, the emergence of novel economic opportunities, and the integration of diverse stakeholder groups in space missions have given rise to fresh technological, legal, and social Space Cybersecurity (SC) challenges [1]. Cyberattacks targeting satellites, ground stations, or data transmissions can threaten critical infrastructure on Earth, disrupting communication networks, financial systems, and even navigation capabilities. Such insecurities jeopardize economic growth, exacerbate societal risks, and potentially threaten inter/national security [2]. For example, the February 24, 2022, Viasat KA-SAT network attack, which left thousands in Europe offline, highlighted the vulnerability of satellite infrastructure as a potential target for cyber attackers [3]. Likewise, the 2022 breach of SpaceX's Starlink terminals underscored the advanced nature of cyberattacks targeting the space industry [3]. The array of cyber threats targeting satellite systems is vast and varied, encompassing attacks such as denial of service, hardware backdoors, privilege escalation, sensor injection, jamming, eavesdropping, bespoke malware, payload hijacking, metadata analysis, replay attacks, signal injection/hijacking, generic malware, social engineering, physical access, and data corruption [4–6]. Nonetheless, there is no standard classification or taxonomy of what constitutes a cyber incident; therefore, there is no definitive threat list [7]. Any single incident or sequence of events that imperils the availability, authentication, reliability, confidentiality, robustness, integrity, and trustworthiness of space digital information flow in the space mission must be secured [8], necessitating space-centric cybersecurity strategies.

It is often argued that orthodox Cyber-Physical System (CPS) cybersecurity solutions could immediately remedy SC challenges [9–11]. However, these solutions are insufficient to address space systems' cybersecurity. The reasons include a **unique environment**: space systems operate in extreme conditions such as temperature, radiation, and vacuum, making conventional terrestrial cybersecurity solutions less effective or inapplicable [12]. **Longevity of satellites**: satellites

* Corresponding author.

https://doi.org/10.1016/j.ijcip.2024.100724
Received 5 July 2024; Received in revised form 18 September 2024; Accepted 4 November 2024
Available online 13 November 2024

have extended lifespans, and their technology may become outdated, making cybersecurity upgrades challenging and costly. **Limited physical access:** once a satellite is launched, physical access is nearly impossible, complicating maintenance or updates to cybersecurity measures. **Real-time constraints**: space systems require real-time operations and cannot tolerate latency introduced by traditional cybersecurity measures like encryption or additional authentication steps. Moreover, the **highly specialized nature** of space systems implies that traditional cybersecurity solutions might not fully address their unique vulnerabilities and requirements. This also makes **patching and updates** challenging due to limited satellite access, real-time operational demands, technology obsolescence, and harsh space environments [13].

Simultaneously, the **dual-use nature** of many satellites, serving both civilian and military purposes, adds to the complexity of implementing effective cybersecurity measures that cater to various stakeholders [14]. For instance, **stakeholder fragmentation** involves various actors with different objectives, like governments and private firms. This complexity complicates the establishment of unified cybersecurity standards, necessitating improved collaboration and coordination to tackle unique risks. **Geopolitical considerations** subject space systems to international legal frameworks, complicating the implementation of uniform cybersecurity measures due to differing legal, political, and technical factors [15]. **Intellectual property** protection is vital for promoting innovation, investment, and industry growth while addressing technology theft concerns. **Memory and computation constraints** on space systems affect the effectiveness of security measures. Simultaneously, **uncertainty** in SC arises from unpredictable cyber threats and challenges in the space environment, making securing critical infrastructure and networks difficult. Fig. 1 illustrates the unique challenges for space systems' cybersecurity. Nevertheless, the multi-faceted nature of SC necessitates a comprehensive evaluation encompassing socio-technical aspects intertwined with space missions.

While space cybersecurity research has recently drawn attention, it often remains fragmented, focusing on individual facets within the space or cyber domain without fully acknowledging the interconnected nature of space components, threats and vulnerabilities [16]. As such, the existing literature lacks a comprehensive analysis of space cyber-attack vectors. This research problem is further amplified by the limited applicability of existing security frameworks and solutions to SC's unique challenges. For instance, there is a dearth of mitigation strategies specifically designed to address the challenges of satellites' unique environment and longevity to ensure mission success and minimize technical failures stemming from cyberattacks on satellite constellations [13,17]. Similarly, the limited physical access and real-time constraints add complexities to updating the software and firmware of space assets and often require multiple fly-bys [13]. The dual-use nature of the space infrastructure, their memory and computation constraints, and the fragmentation of stakeholders pose risks in managing security keys and demand scalable and efficient key management systems [13].

Further complicating the landscape are unresolved legal and regulatory issues. The legal status and internet access capabilities of Low Earth Orbit (LEO) satellites remain contentious [18], highlighted by the recent request from the US Department of State for SpaceX to turn off specific features in Ukraine, reflecting concerns about adherence to international laws prohibiting military use of outer space. This begs the question of whether LEO satellites should be considered integral parts of global telecommunications infrastructure or require distinct cybersecurity regulations. Therefore, it is essential to develop a comprehensive understanding of space cyberattack vectors that recognise the evolving landscape of cyber threats, critically evaluate the effectiveness of legacy solutions and frameworks, and propose research direction contributing to multi-layered SC defence mechanisms encompassing both technical and legal-regulatory dimensions.

The study makes the following contributions:

- **Comprehensive Analysis of Space Cyber-Attack Vectors:** We meticulously examine the vast scope of potential attack vectors across all segments of space infrastructure, including ground, space, user, cloud, communication channels, and supply chains. The unique aspect of these vectors in space necessitates a holistic analysis to address their complex nature and potential impact on space missions.
- **Development of Effective Mitigation Strategies**: We propose a multi-faceted strategy that extends beyond technical solutions to include regulatory frameworks, standards, and workforce development, aiming to enhance cybersecurity across the entire space operations lifecycle, focusing on addressing SC's distinct requirements.
- **Exploration of Emerging Technologies and Regulatory Needs:** We highlight the value of investigating promising fields like intrusion detection systems, blockchain-based access control, quantum technologies, and space awareness systems. Additionally, we call on researchers to analyse the establishment of international standards, Key Performance Indicators (KPIs), norms of behaviour, and clear liability frameworks for the age of space commercialization.

These contributions offer socio-technical insights, research directions and a comprehensive framework for future SC studies. Similarly, for technology developers they serve as reference for devising novel solutions to address critical security challenges. Furthermore, they

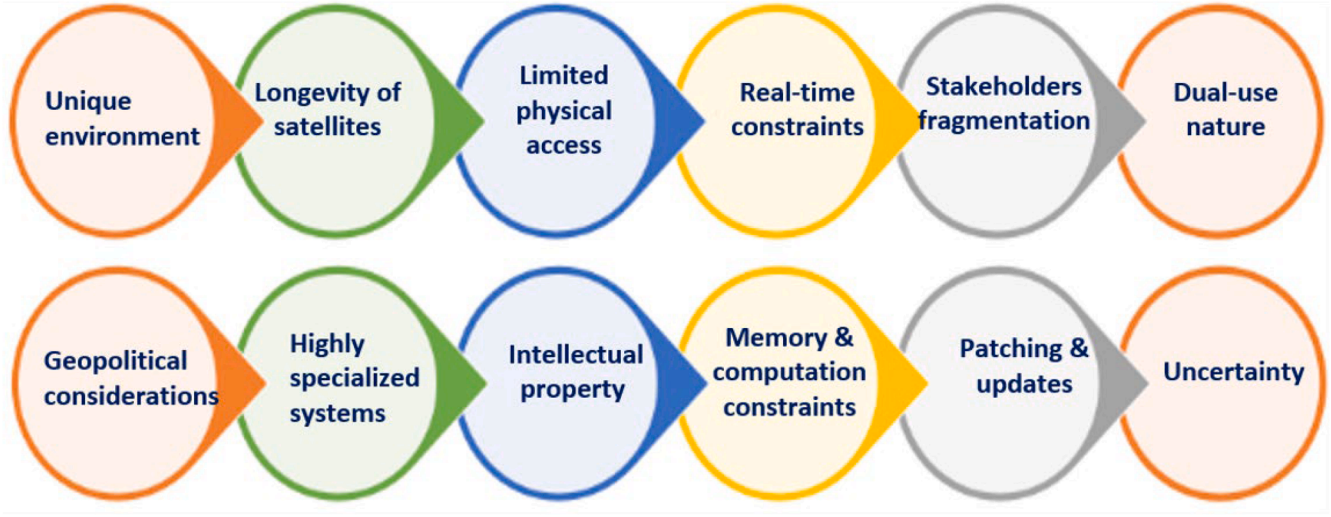

Fig. 1. Unique challenges for space systems' cybersecurity.

support decision-makers' informed policy development and facilitate the creation of a robust and sustainable SC framework.

The rest of the paper is structured as follows: Section 2 delineates the methodology employed. Section 3 details the state-of-the-art literature on SC, offering a comprehensive overview of cyber-attack vectors. This section also discusses counterstrategies and potential mitigation techniques. Section 4 outlines the SC research directions.

2. Research method

The study employed a narrative literature review approach to identify and map the current state of SC and identify areas for future research. The literature was identified by searching multiple academic databases, such as Web of Science, SCOPUS, TRID, and Google Scholar. Using a combination of Boolean operators, the following keywords were searched (up to January 25, 2023):

- Space cybersecurity
- Satellite and cybersecurity
- Space cybersecurity policies and regulations
- Threats and vulnerabilities in satellite communication systems
- Cybersecurity in satellite-based navigation systems (e.g., GPS, Galileo, and GLONASS)
- Cyberattacks on space infrastructure and their implications
- Protecting space assets from cyber threats
- Space situational awareness and cybersecurity
- The role of the public and private sectors in securing space infrastructure
- International cooperation in space and cybersecurity
- Cybersecurity best practices for satellite operators
- Developing secure communication protocols for space missions
- Socio-technical aspects of cybersecurity

Our initial academic database search yielded 151 peer-reviewed articles. Applying inclusion/exclusion criteria based on abstract relevance, we identified 111 relevant articles related to SC. Interestingly, the analysis revealed a significant level of consistency in publication sharing across different platforms within the SC domain. Consequently, we removed duplicates and focused on 61 articles that offered an in-depth analysis of socio-technical trends within SC. Examining the references of these articles further identified 11 additional relevant articles. This resulted in a final set of 72 articles for systematic review. Table 1 illustrates the literature identification and selection process.

Additionally, relevant industry reports and technical papers from sources such as The Space Review, SpaceNews, and Space.com were consulted. Websites of organizations like the European Space Agency, NASA, and international cybersecurity organizations were reviewed for recent publications and news articles on space and cybersecurity. Forward and backward snowballing techniques were used in related articles to conduct an in-depth examination, compile information, and derive pertinent findings for SC. We analysed each of the selected papers to identify critical cyber-attack vectors and counterstrategies. For this, we followed the concept mapping strategy. We developed two concept matrices by reading each paper – one for space cyber-attacks and another for mitigation strategies.

Table 1
Literature identification and selection protocol.

Identification	Database: Web of Science, SCOPUS, TRID, Google Scholar Period: up to January 25, 2023 Search String: Using a combination of Boolean operators and the keywords mentioned above, such as "space AND ["cybersecurity" OR "cyber security" OR "cyber-security"]				
	Result	Web of Science n=52	SCOPUS n=41	TRID n=9	Google Scholar n=49
Screening	After removing duplicates	n=151			
	Determining relevancy based on abstract	n=111			
Selection	After quality inspection and removal of duplicates	n=61			
	After analyzing the reference chain	n=72			

Moreover, to suggest areas for further research, the VOSviewer application was used to visualize the major themes, relationships, and occurrences of the 72 selected papers via infographics [19]. The network visualization for thematic clusters of the articles is shown in Fig. 2. The minimum number of occurrences for a keyword (items) is considered 10, bringing the total number of keywords chosen to 581. Items are represented by a label and, by default, a circle, and the size of the label and circle for an item is dictated by the object's weight. The greater the item's weight, the bigger the label and circle.

The primary cluster (in red) revolves around space cybersecurity, addressing various aspects like computer security, protection, risk management, awareness, cybercrime, policy development, and resilience. The second cluster (in green) delves into algorithms, datasets, and features related to space cybersecurity. The third cluster (in yellow) examines the space domain's internet, IoT, quantum computing, and consumer applications. Lastly, the fourth cluster (in purple) concentrates on protocols, computation, schemes, and codes in space missions.

The holistic network visualization provided by Vos Viewer identified key areas needing further exploration, such as the interconnectedness between space cybersecurity and the digital economy within the emerging New Space sector. This necessitates calls for research on the following:

- Cyber-attack vectors: How do digital transformation and the involvement of diverse stakeholders in space missions create new vulnerabilities across all mission phases? What attack vectors emerge from these new economic opportunities? We explore these questions in detail in subsequent sections.
- Space infrastructure vulnerabilities: Despite growing threats, research on cyber-attack vectors targeting critical space infrastructure and their mitigation methods remains limited.
- Legal and socio-technical aspects: The influence of legal frameworks on space cybersecurity and the interplay with cybercrime require deeper investigation to build robust legal and security measures.

3. State-of-the-art

This section is divided into three subsections. The initial subsection provides a global overview of space cybersecurity. The subsequent subsection delves into an extensive examination of cyber-attack vectors, covering the ground, space, user, cloud, communication channels, and supply chain. The final subsection discusses counterstrategies and potential mitigation techniques in space cybersecurity.

3.1. Overview of existing studies on space cybersecurity

The evolution of space technology has become integral to global critical infrastructure, enabling communication, safe air travel, maritime trade, weather monitoring, environmental surveillance, financial services, and defence systems [20]. This journey of space technology unfolds across three generations, each representing a distinct era of advancement and innovation [21], as depicted in Fig. 3. The first generation (1957–1980) was marked by the U.S. – Soviet space race, giving rise to space agencies and the launch of pioneering communication satellites, meteorological initiatives, and earth observation programs. The second generation (1981–2000) witnessed increased

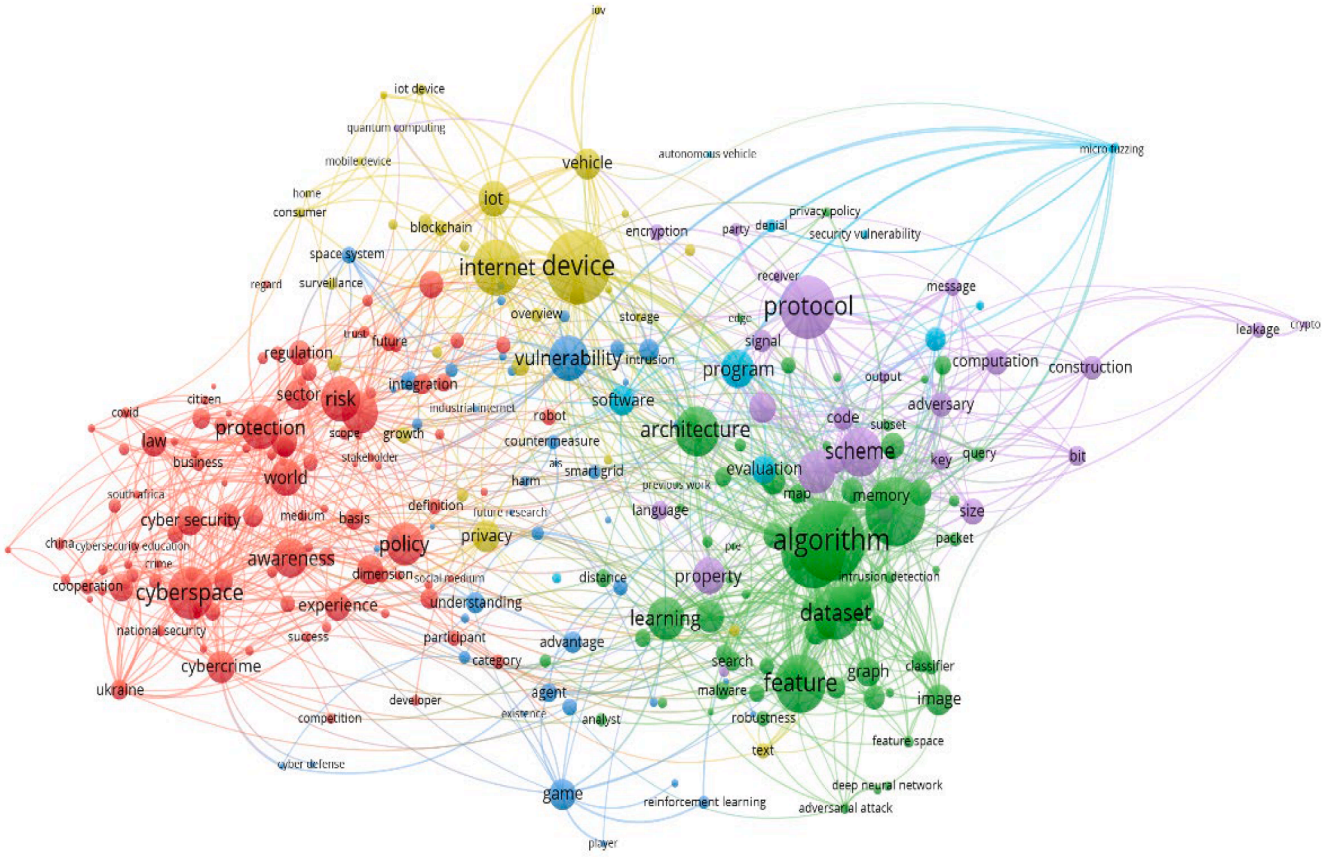

Fig. 2. Network visualization illustrating the occurrences of thematic keywords related to space cybersecurity.

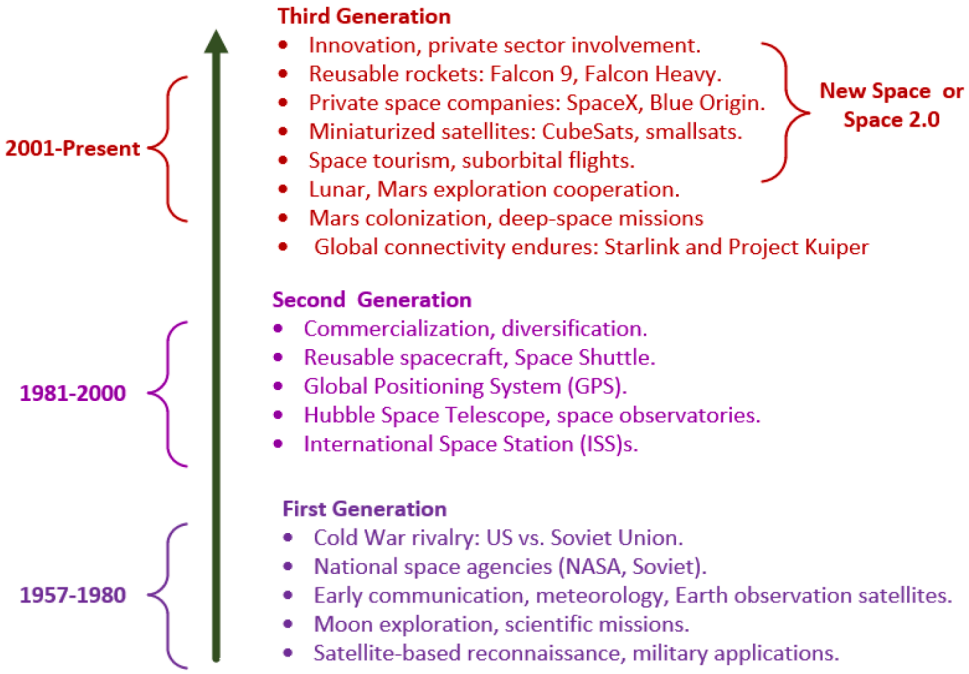

Fig. 3. Space transformation (Author's synthesis).

commercialization and diversification, introducing reusable spacecraft, GPS, the Hubble Space Telescope, commercial satellite services, and the International Space Station.

The ongoing third generation (2001–present) is characterized by innovation, private sector involvement, intergovernmental organisations (such as the European Space Agency) and the democratization of space technology [22,23]. It has seen advancements like reusable rocket technology, the prominence of private space companies such as SpaceX

and Blue Origin, the miniaturization of satellites, the emergence of space tourism, global collaboration on lunar and Mars missions, and ambitious plans for Mars colonization, collectively termed "New Space" or "Space 2.0,".

The interest in cybersecurity aspects of space missions has significantly increased recently in both the academic and industrial sectors, demonstrating the field's growing significance [24]. The authors in [9] examine satellite cybersecurity threats to understand adversaries' motivations and characteristics, highlighting that ground and radio frequency communications have been preferred targets. Dunn Cavelty and Wenger [10] examine the use of cyberspace in conflict settings, political responses by state and non-state actors, and the evolving shared responsibility for cybersecurity in an increasingly trans-sectoral and transnational governance space. Similarly, Pavur and Martinovic [4] explore the importance of securing both emerging and legacy satellite missions amidst rapid changes in the space industry while arguing that the satellite systems security community has largely overlooked space technology.

The increased integration between space and cyberspace leads to numerous cybersecurity challenges for space infrastructure. Lin, Henry [25] demonstrates a potential attack vector using Software-Defined Radios (SDR), highlighting the need to identify and address such vulnerabilities to improve security and prevent disruptions in the global space enterprise. Moreover, the authors of [2] discuss the potential risk of simultaneous satellite failure due to cyber-attacks, highlighting the dependency on satellite data and the economic damage such a collapse could cause. The authors explore technical countermeasures like rapid response programs and policy-oriented measures, focusing on transparency and confidence-building measures to address this growing threat.

Rementeria [26] explores the space movement's effects and outer space commercialization on established power hierarchies. As more participants enter the low-orbit sector, the author contends that the dominance of a few space-centric states will probably persist only in the short-to-medium term. The authors of [27] discussed the rapid growth of Low Earth Orbit (LEO) satellite systems and highlighted the unique vulnerabilities and countermeasures to enhance the security of LEO satellite communication systems. Simultaneously, the surge in satellite constellations may shift the focus to the space segment, necessitating a discussion on key technology advancements and open security issues in the satellite industry [9]. Moreover, the authors in [11] discussed that the rise of global internet access from LEO brings cybersecurity vulnerabilities, and international space law remains ambiguous regarding outer space cybersecurity. It proposes a multistakeholder international legal regime for space cybersecurity, emphasizing that international cooperation is crucial for consistent cyberspace protection in line with the core principles of collaboration in space.

Kirshner [28] discussed the adoption of Model-Based Systems Engineering (MBSE) in space systems development. The author proposes a methodology using MBSE functionality to verify and validate cybersecurity for cyber-physical space systems. Similarly, Shahzad and Qiao [29] proposed a cyber resilience framework for critical space infrastructure, emphasizing the importance of addressing risks in digitally connected space infrastructure. The authors call for further collaboration to understand and mitigate space-asset-reliance disruption risks. In addition, the authors of [1] argue that an immediate need exists to develop a flexible, multilateral space cybersecurity regime through international cooperation and industry-led standards to respond effectively to space-based cyber threats.

The space domain is becoming increasingly congested, contested, and competitive, with growing threats to societies and critical infrastructure. Cyberattacks on satellites, which could disrupt critical infrastructure and services, are a significant concern as more commercial satellites enter the space domain and a broader range of actors join the space race [30]. Kulesza and Akcali Gur [18] highlighted that LEO satellites providing internet access in conflict zones, such as Ukraine, raise international law questions regarding accessibility, funding, and military use. The paper explores policy options for governments, recommends using UN sustainable development goals as guiding principles for satellite-facilitated telecommunications infrastructure, and emphasizes the importance of addressing cybersecurity concerns. Ukhanova [31] highlighted the case of Japan, which is heavily reliant on its information infrastructure. It has developed a complex information security, cybersecurity, and cyber defence strategy, focusing on proactive actions and enhancing reactive capabilities. An essential aspect of Japan's cybersecurity strategy involves taking proactive measures while simultaneously improving its reactive abilities, which include the appropriate development of containment and sustainability capabilities.

Fleming, Reith [32] presented the cybersecurity supply chain framework to assess and select commercial satellite contracts, ensuring security for their supporting components. The framework streamlines requirements for small businesses, extends essential requirements to Commercial-Off-The-Shelf (COTS) suppliers, and incorporates a scoring process to assess subcontractors' cybersecurity capabilities. Moreover, the authors in [33] analyzed space information networks' characteristics and cybersecurity requirements, which are vulnerable to cyberattacks due to their fixed positions and standardized message formats. The authors proposed a new situation awareness and information defence strategy combining multi-domain approaches for space information security. Building upon previous research, this paper addresses a critical gap in the literature by systematically synthesizing potential attack vectors across all space infrastructure segments (ground, space, user, cloud, communication, and supply chains). Additionally, the paper outlines comprehensive mitigation techniques for these cyber-attack vectors and identifies emerging socio-technical challenges in SC. Table 2 summarises studies examining various aspects of SC.

3.2. Space cyber-attack vectors

Technological advancements, multistakeholder fragmentation, and increased investment have broadened the space cybersecurity threat landscape. Consequently, futuristic space missions are surrounded by a force field of cybersecurity challenges. Potential cyberattack vectors include the ground segment, space segment, user segment, cloud segment, communication channel, and supply chain, as depicted in Fig. 4. These six pillars are derived through "meta-synthesis", which refers to the in-depth review and integration of findings from qualitative SC literature [34,35]. In the following subsections, each pillar is discussed in detail.

3.2.1. The ground segments

The ground segment of the space system enables control and monitoring of space assets via terrestrial networks and infrastructure [36]. It comprises ground stations, Telemetry, Tracking, Command System (TT&CS), a mission control centre, data processing units, and a user terminal. Ground stations are equipped with antennas and communication equipment for satellite control. TT&CS monitors the satellite's health and position, while a mission control centre oversees operations. Data processing and storage facilities handle the data collected by satellites, and communication networks connect all ground segment components. User terminals provide access to satellite services, and various support systems ensure smooth operation and maintenance. The potential cyberattack vectors include computer network exploitation, data corruption or modification, unpatched or outdated software, and physical access attacks [9,37].

Exploiting a computer network entails compromising the network connected to a ground station, analogous to attacks on enterprise IT networks. Attackers could use poorly configured or vulnerable technologies or phishing to gain unauthorized access to ground control stations and disrupt or manipulate space assets, endangering satellite missions and services. A compromised command for a spacecraft could result in catastrophic loss. Similarly, unpatched, out-of-date, or legacy

Table 2
Overview of space cybersecurity studies.

Purpose of the Study	Methodology	Evaluated parameters	Key aspects explored	Limitations
Cyber security in New Space [9]	Literature Review and conceptual Modelling	Analysis of threats, key enabling technologies and challenges	Satellite cybersecurity threats, motivations of adversaries, preferred targets	Lack of emphasis on the importance of regulation in compliance with cybersecurity protocols
Cyber Security Politics [10]	Literature Review	Trans-sectoral and transnational governance space	Use of cyberspace in conflict, political responses, shared responsibility for cybersecurity	Lack of assessment of technological aspects in different segments of space missions
satellite cyber-security [4]	Analysis of Secondary data	threat matrix toolbox	Importance of securing emerging and legacy satellite missions, overlooked space technology	Lack of focus on cybersecurity of the cloud segment, an important part of space missions
Defending Small Satellites from Malicious Cybersecurity Threats [25]	Simulation	Software-defined radios	Potential attack vector using Software-Defined Radios, need for vulnerability identification and prevention	Focus limited to a specific simulated scenario, lacks practical considerations in space mission data flow
Satellite data loss [2]	Survey	Rapid Response programs, Transparency and Confidence Building Measures	Risk of simultaneous satellite failure due to cyber-attacks, dependency on satellite data, economic damage	Lack of explicit analysis of software and hardware threats from COTs suppliers.
Power Dynamics in the Age of Space Commercialisation [26]	Literature Review	space-centric power dynamic	Effects of space commercialization on power hierarchies, persistence of dominance by space-centric states	Lacks dynamic assessment of small hardware supplier roles in space commercialization
Security and Reliability [27]	literature review and simulations	Reliability and cybersecurity	Growth of Low Earth Orbit satellite systems, vulnerabilities and countermeasures for LEO satellite communication	Lack of compliance with cybersecurity protocols and assessment of hackers' capabilities
Legal Issues regarding Cybersecurity in Outer Space [11]	Literature review	Outer space regulation	Rise of global internet access from LEO, ambiguity in space law, multistakeholder legal regime for cybersecurity	Focus solely on outer space regulation, lack of analysis on cellular-space network laws
Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions (This Study)	Literature review	Cross-disciplinary areas that seamlessly integrate space and cyber domains	Provides a thorough analysis of cyber-attack vectors, covering the ground, space, user, cloud, communication channels, and supply chain Outlines counterstrategies and potential mitigation techniques Outlines the research directions for space mission cybersecurity, emphasizing technological drivers for developing and implementing solutions and regulatory/ operational frameworks	The research does not investigate potential quantitative assessment models that could offer insights into SC's long-term and short-term implications.

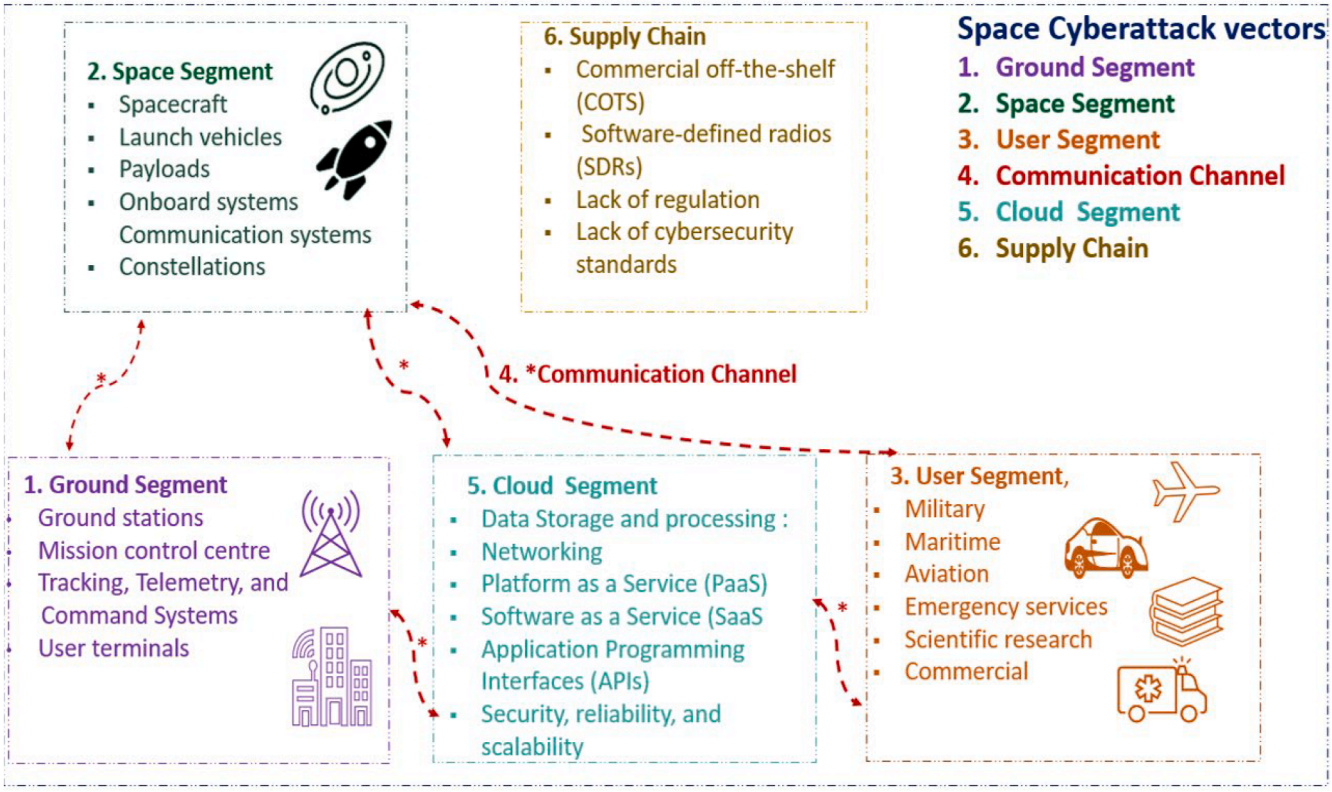

Fig. 4. Space cyber-attack vectors (Source: Authors' synthesis).

platform software is an attack surface that leaves the program vulnerable to cyberattacks. For instance, Symantec Corporation reported that a Chinese cyberattack compromised satellite operators, defence contractors, and telecommunications companies in the United States and Southeast Asia [38]. The compromised satellite control systems allowed the attackers to orbit satellites and halt data transmission.

Furthermore, physical attacks such as unauthorized access to ground stations and other physical assets can turn off the ground station, directly jeopardizing the operation of the space mission and seizing control of the space assets and their services without technically attacking the systems. A NASA report [39] detailed the theft of an unencrypted notebook computer and the subsequent loss of command and control algorithms for the International Space Station. In 2007 and 2008, ground stations took over two NASA satellites [4,40,41]. Nonetheless, these threats typically remain consistent throughout a satellite's life cycle. They can be either active (direct actions to compromise a system) or passive (eavesdropping).

3.2.2. The space segment

The space segment of a space system typically encompasses spacecraft (satellites, space probes), launch vehicles (rockets), payloads (scientific instruments, cameras, communication devices), onboard systems (power, propulsion, attitude control, thermal control), and communication systems [42]. Spacecraft are vehicles designed to operate in outer space for various purposes, such as communication, earth observation, or scientific research. Rockets transport these spacecraft to outer space, carrying payloads from the Earth's surface. Payloads consist of scientific instruments, cameras, and communication devices essential for specific missions. Onboard systems ensure proper spacecraft functionality, including power generation, propulsion, attitude control, and thermal control. Lastly, communication systems include telemetry, tracking, and command infrastructure, facilitating communication between spacecraft and ground control stations.

There are three distinct types of satellite orbits: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO) [43]. LEO satellites are positioned closer to Earth, typically around 500 to 2000 kilometres above the surface. They offer shorter communication latency and require less power for signal transmission, making them ideal for earth observation, weather monitoring, and low-latency communications applications. MEO satellites are situated at higher altitudes, generally between 2,000 and 36,000 kilometres, and are used for navigation systems like GPS, providing more extensive coverage than LEO satellites. GEO satellites orbit approximately 36,000 kilometres, where their orbital period matches Earth's rotation, causing them to appear stationary from a ground observer's perspective. These satellites are commonly used for communication, broadcasting, and weather observation, delivering continuous coverage over vast areas.

Space-based software and hardware vulnerabilities can affect satellite operations and security controls [44]. However, gaining control of a satellite is challenging, as compromising the telemetry, tracking, and command lines demands high skill and knowledge. Attackers can combine multiple channels, such as software flaws and signal replay, to seize control. Even well-protected institutions like NASA have experienced satellite commandeering [45]. Spacecraft rely on on-orbit maintenance and power supplies for critical components for mission success. Any tampering or compromise of orbital dynamics, such as attitude control functions, may lead to mission failure [37].

Clusters and constellations of satellites may experience cyberattacks targeting their communication, control, and coordination systems, leading to disrupted mission objectives, loss of satellite control, or even collisions due to jamming, spoofing, denial of service, unauthorized access, and malware infections. Furthermore, attackers could exploit the increased attack surface to disseminate malware or tamper with control systems across multiple satellites, resulting in cascading effects and putting the entire mission at risk. Other potential cyberattacks encompass command intrusions manipulating controls, malicious payload interference, and denial of service attacks.

Cybersecurity is crucial for preventing unauthorized control in space because assets like satellites are inaccessible for hardware maintenance or repair once deployed. Cyberattacks can induce operational errors, potentially allowing adversaries to seize control of the satellite and its strategic capabilities. Such scenarios are hazardous, as compromised satellites can pose threats akin to anti-satellite missiles, endangering the safety of other space assets and terrestrial infrastructure reliant on satellite services. In 1998, the ROSAT satellite sustained damage from pointing towards the sun due to an operational error caused by a command outside its safe limits, which was suspected to be a cyberattack by Russia [46].

3.2.3. The user segment

The space mission user segment encompasses government, military, commercial, maritime, aviation, emergency services, and consumer markets [1]. These end users access satellite system-provided information and services through user terminals. Essential components of the user segment include antennas and receivers for establishing communication links with satellites, as well as modems and transceivers for converting digital data into radio frequency signals and vice versa. Signal processing and data handling equipment manages data received from or transmitted to satellites, while positioning and tracking equipment calculates user positions in satellite-based navigation systems. Furthermore, user interfaces and displays facilitate interaction with satellite services and data visualization, supported by software and firmware that control hardware components and provide user interfaces.

The user segment is vulnerable to various cyberattacks. Potential cyberattacks include data breaches involving unauthorized access to user terminal equipment, compromising service integrity and confidentiality. Attackers can introduce malware or ransomware into terminal user equipment, affecting functionality, stealing data, or demanding ransom for restoration operations. Denial of service (DoS) attacks overwhelm terminal user equipment with excessive traffic or requests, causing disruptions. Man-in-the-middle attacks intercept communication between user terminals and satellites, potentially manipulating data or gaining unauthorized access to sensitive information. Security analyses of satellite user terminals in [47,48] revealed hard-coded credentials, backdoors, ineffective authentication mechanisms, and insecure protocols by various vendors.

Physical access to user terminals can facilitate a range of cyberattacks. Additionally, a system capable of executing software-defined GPS spoofing is simple to develop and inexpensive, costing approximately $1000 [49]. It is believed that Iranians effectively captured an American RQ-170 Sentinel drone in September 2011 by reconfiguring GPS coordinates so that the drone landed in Iran instead of its base in Afghanistan [50].

3.2.4. The Communication Channel

Establishing communication links (both uplink and downlink) between the space and ground segments relies on radio frequency waves, typically transmitted at Gigahertz (GHz) frequencies [51,52], as illustrated in Table 3. The communication link between the space and ground segments is particularly vulnerable to cyberattacks. Potential cyberattacks on the communication segment in satellite missions include jamming and interference (disrupting communication links between satellites and ground stations); spoofing (sending fake signals to deceive receivers); data breaches (unauthorized access to sensitive information); malware and ransomware (infecting systems with harmful software or demanding ransom for data release); DoS attacks (overwhelming systems with excessive traffic or requests); and man-in-the-middle attacks (intercepting and potentially altering communications between satellites and ground stations).

Table 3
Satellite frequency bands, applications, and limitations.

Frequency Band	Frequency Range	Typical Applications	Limitations
L-band	1-2 GHz	Satellite phones, mobile communications, and GNSS signals (e.g., GPS).	Limited bandwidth, potential interference.
S-band	2-4 GHz	Weather radar systems, satellite phones, and mobile communication systems.	Limited bandwidth, susceptible to interference.
C-band	4-8 GHz	Satellite television, internet services, and telecommunication systems.	Susceptible to interference, larger antennas are required.
X-band	8-12 GHz	Military communication, weather radar systems, satellite-based remote sensing.	Limited bandwidth, susceptible to rain fade.
Ku-band	12-18 GHz	Satellite television broadcasting, internet services, remote location data communication.	Susceptible to rain fade, potential interference.
K-band	18-27 GHz	High-capacity data transmission, high-resolution radar systems, and inter-satellite links.	Susceptible to rain fade and atmospheric absorption.
Ka-band	27-40 GHz	High-speed satellite internet, high-definition television broadcasting, and inter-satellite communication.	Highly susceptible to rain fade, atmospheric absorption
V-band	40-75 GHz	High-speed satellite internet, inter-satellite communication, satellite-based remote sensing.	Susceptible to rain fade, atmospheric absorption, and limited range.
W-band	75-110 GHz	High-capacity satellite communication, inter-satellite links, imaging radar systems	Highly susceptible to rain fade, atmospheric absorption, and limited range.

3.3. Performance evaluation metrics for space communication

A robust communication link must incorporate seven facets of security and safety for a cyber-secure space mission: availability, authentication, reliability, confidentiality, integrity, robustness, and trustworthiness [53], as illustrated in Fig. 5. Availability is the primary goal for facilitating real-time space networking, and attacks such as DoS, black-hole, spamming, grey-hole, jamming, flooding, or wormholes could impact it [54]. Authentication prevents malicious access by implementing restrictions on verifying space-operation nodes, with potential cyberattacks including GPS spoofing, tunnelling, free riding, message tampering, replication, Sybil, impersonation, and wormhole attacks [55]. Reliability ensures the confidence of information flow (commands, data, and signals), such as slight and sensor attacks [56]. Confidentiality protects space-intellectual property from unauthorized disclosure, with potential attacks including man-in-the-middle, eavesdropping, and traffic analysis [57]. Integrity ensures data cannot be altered without permission, and potential attacks include masquerading, illusion, replay, and unauthorized software modifications [58,59]. Robustness refers to the space communication framework's ability to perform well in the face of disruptions, such as incorrect or unforeseen inputs. Trustworthiness of the data flow fosters trust among stakeholders in the level of safety and security of the space mission.

3.3.1. The cloud segment

The cloud segment processes and analyses satellite data, facilitating communication and coordination between satellite operators, service providers, and end users. Web-based interfaces and Application Programming Interfaces on cloud platforms make satellite data and applications more accessible and easier to adopt [60]. The cloud segment improves efficiency, flexibility, and accessibility for space communication [26,61] by utilizing shared resources and economies of scale to deliver cost-effective solutions for growing data volumes. Companies like Planet, KSAT, and Amazon have already adopted cloud-based technologies, with satellite sector companies like DigitalGlobe, BlackSky, and Spire Global among their customers [9,62]. Moreover, cloud service providers protect satellite data and communication channels with robust security and backup systems, ensuring reliability and

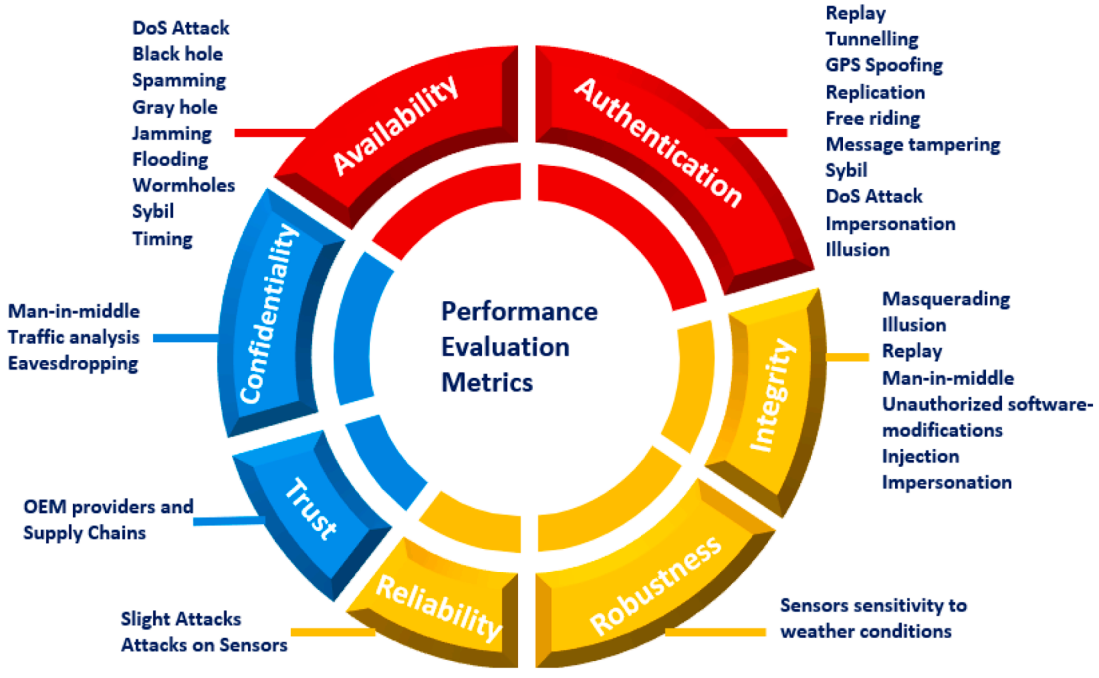

Fig. 5. Space cyber-attack classification under security performance evaluation metrics (Source: Author's synthesis).

uptime. Furthermore, the space-cloud segment of innovation will be a crucial facilitator in the application of Industry 4.0 [63]. However, the cloud segment of space communication is susceptible to various cyber-attacks, including data breaches, account hijacking, DoS attacks, insider threats, Advanced Persistent Threats (APTs), supply chain attacks, and misconfigurations [64,65].

3.3.2. The supply chain

The proliferation of COTS satellite components has significantly contributed to the growth of the small satellite market. Pre-built satellite flight hardware availability reduces acquisition costs, allowing New Space players to take on more technical and commercial risks. For instance, a fully assembled 1 kg "Cube Satellite" can now be purchased for $16,000 [66]. However, the increasing complexity of space assets and reliance on COTS components opens opportunities for malicious actors to introduce vulnerabilities into the supply chain, posing security risks[66]. Simultaneously, Software-Defined Radios (SDRs), adaptable communication systems in which software replaces standard hardware components for simple updates and reconfiguration, have made such attacks easier to execute. In addition, the lack of regulation and cyber-security standards in e-space products increases the number of cyber-attack vectors [7,67].

The crucial aspects of the supply chain in space cybersecurity include **Hardware and Software Vulnerabilities**: components sourced from various suppliers could have built-in vulnerabilities or backdoors, which cybercriminals can exploit to compromise the security of space systems. Similarly, outdated COTS software on a system creates a known attack surface. Common Vulnerabilities and Exposures (CVE) regularly updates lists disclosing COTS or open-source software vulnerabilities [9]. **Counterfeit Components**: using counterfeit or substandard parts in space systems can lead to failures, reduced performance, and increased security risks. **Dependency on Third-Party Services**: reliance on external services for satellite control, data processing, or communication can expose space systems to additional risks if these services are compromised or experience downtime. **Insider Threats**: malicious insiders within the supply chain can intentionally introduce vulnerabilities or facilitate cyberattacks on space systems. **Geopolitical Risks**: dependence on suppliers or service providers from regions with political instability or adversarial relationships can pose risks to the security and continuity of space systems and services.

3.4. Counterstrategies and potential mitigation techniques

In the evolution of SC, there have been three distinct phases [8,68]. The **System-Centric** period (1960s–1980s) marked the advent of networked systems and mainframe computers with rudimentary security measures like password protection and access controls. The **Data--Centric** era (1990s–2000s) saw the widespread adoption of the Internet and the World Wide Web, leading to the development of firewalls, antivirus software, and encryption and increasing public awareness of cybersecurity and cybercrime. The current **Organization-Centric** phase (2010–present) is characterized by pervasive connectivity, cloud computing, and a network of IoTs. This phase employs advanced techniques such as Artificial Intelligence (AI) in cybersecurity while facing growing concerns around state-sponsored attacks, ransomware, and critical infrastructure protection.

Satellite security frameworks play a crucial role in this endeavour, and various approaches have been proposed. One approach advocates dividing missions into distinct phases [69] and applying specialized cybersecurity overlays to each, promoting "security by design." Another links security controls directly to mission types, incorporating generic controls where applicable. A hybrid approach considers both mission-specific attack probabilities and mission phases for more precise threat modelling. While mapping existing IT security controls to satellite systems is common, concerns arise about its effectiveness in accounting for the unique threats and multistakeholder landscape of such systems. In this context, the suitability of established frameworks within the satellite industry, like the NIST Cybersecurity Framework, remains uncertain. The various domains necessitated for an effective SC based on the cyber-attack vectors are discussed below and depicted in Fig. 6. In the following sub-sections, each domain is discussed in detail.

3.4.1. Secure communication protocols

The communication link serves as the primary and expansive attack surface for malevolent entities, capitalizing on vulnerabilities inherent in satellite communication protocols. Such exploitation manifests as a spectrum of threats, including but not limited to jamming, interference, spoofing, tampering, repudiation, and denial of service [70]. Presently employed protocols in space communication, notably Secure Shell (SSH) and Space Communications Protocol Standards (SCPS), exhibit limitations and potential vulnerabilities. These encompass shortcomings in password-based authentication, challenges in key management, susceptibility to Man-in-the-Middle attacks, and potential vulnerabilities in protocol implementation. Significantly, these protocols may inadequately safeguard against insider threats, unauthorized access, and social engineering attacks. This underscores the imperative for additional security measures and best practices to mitigate these multi-faceted risks effectively.

Consequently, implementing robust encryption algorithms and secure communication protocols becomes imperative to fortify data transmission between spacecraft, ground stations, and other mission components. Adopting communication protocols demands carefully considering the trade-off between Quality of Service (QoS) and Cybersecurity [53]. QoS imperatives include real-time data delivery at elevated data rates, secure data movement, interoperability between in-space entities, and seamless end-to-end interactivity between users and space instruments. In contrast, cybersecurity mandates a robust communication link encompassing seven essential facets: availability, authentication, reliability, confidentiality, integrity, robustness, and trustworthiness.

The current fragmented nature of NASA's communications infrastructure, tailored for specific missions, is identified as a limiting factor, necessitating intelligent, interactive, and reconfigurable functions in both hardware and software layers [71]. The proposed architecture based on Internet technologies advocates standardized communication interfaces and autonomous procedural task handling, akin to the operational paradigm of the Internet. Leveraging existing Internet technologies and protocols is advocated for cost savings, enabling direct data distribution without human intervention. These advanced architectures require cutting-edge microwave or optical communication technologies, compact network hardware, and intelligent components for autonomous operation.

In the realm of protocol development, specific attributes such as anti-jamming techniques and secure handover schemes merit consideration [72]. Anti-jamming techniques may find a foundation in spread spectrum, game theory/reinforcement learning, and directive antenna technologies. Secure routing protocols could encompass inter-satellite link routing, flood routing, and cooperative routing, ensuring the integrity and confidentiality of data transmissions. Secure handover schemes, rooted in inter-satellite, beam, and node mobile handovers, further fortify the resilience and reliability of communication links in the dynamic context of space missions.

3.4.2. Intrusion detection and prevention

The implementation of Intrusion Detection Systems (IDS) and subsequent Intrusion Prevention Systems (IPS) is crucial for monitoring real-time network transmissions, identifying unauthorized activities, issuing alerts or taking corrective actions in response to suspicious activities [73,74]. IDS primarily operates through two modalities: misuse detection, which identifies predefined intrusion patterns, and anomaly detection, leveraging learning algorithms to discern abnormal behaviours. Li, Zhou [73] proposes a distributed IDS employing Federated

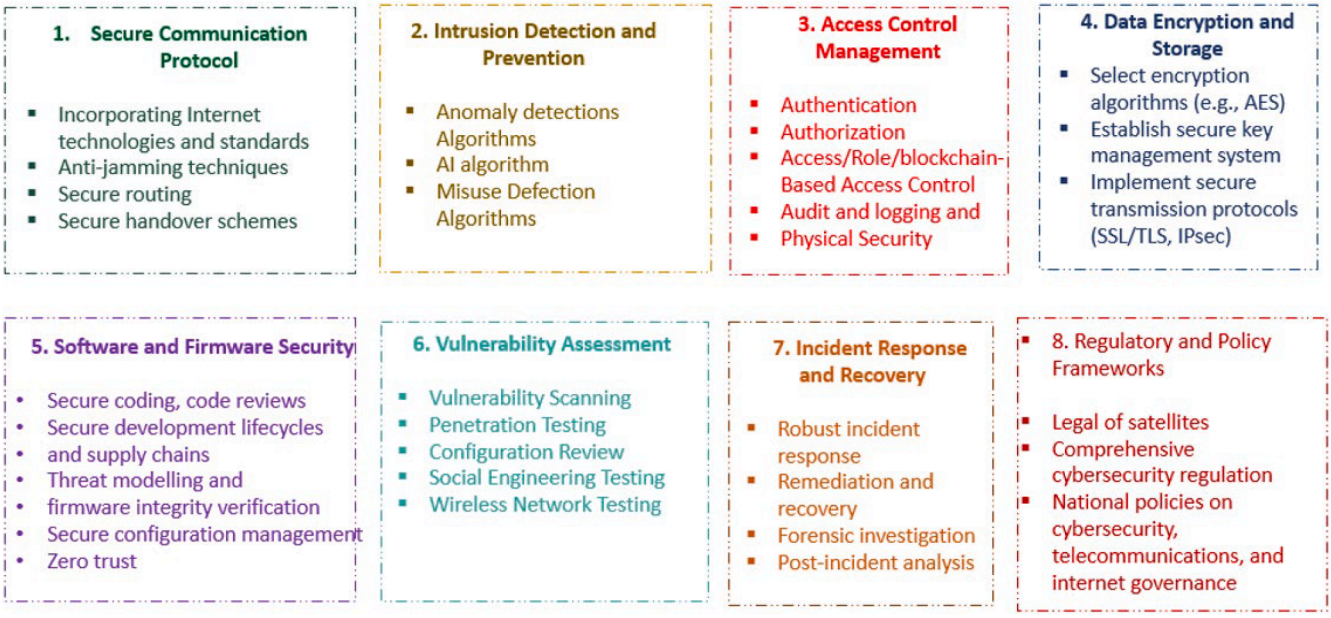

Fig. 6. Counterstrategies and Potential Mitigation Techniques against Space Cyberattack Vectors (Source: Authors' synthesis).

Learning (FL) to address the challenges posed by limited satellite network resources and stringent privacy requirements. This approach optimally allocates resources in each domain to analyze and block malicious traffic, focusing on countering distributed DoS attacks.

Thebarge, Henry [75] employs penetration testing on a cube satellite to delineate potential attack scenarios, subsequently comparing them with analogous terrestrial attack patterns. This analysis informs the discourse on the implementation of onboard intrusion detection systems tailored for satellite components. Additionally, a survey conducted by Diro, Kaisar [76] recommends the integration of stream-based and graph-based methodologies for dynamic anomaly detection in the context of space, further enhancing the sophistication of spaceborne security measures. Similarly, Al-Rubaye and TÜRKBEN [77] explored the application of AI to detect cybersecurity threats in ad-hoc networks. The results demonstrate that machine learning algorithms remarkably detect and effectively classify diverse cyber threats, such as DDoS attacks, malware infiltrations, and attempted unauthorized access.

3.4.3. *Access control management*

Given the diverse array of stakeholders engaged in missions, a pivotal avenue for mitigating security risks within the space system entails implementing robust access control management strategies. This necessitates the deployment of rigorous authentication mechanisms and access control measures to ensure that only duly authorized personnel can access critical systems and data. Critical dimensions of Access Control Management in satellite communication encompass multifaceted elements, such as Authentication (the process of verifying the identity of users or devices); Authorization (the determination of access privileges granted to authenticated users or devices); Role-Based Access Control (the implementation of access control policies based on predefined roles assigned to users or devices); Access Control Lists (the specification of specific permissions for individual users or devices); Audit and Logging (the continuous monitoring and recording of access control events and activities); and Physical Security (the implementation of tangible security measures to safeguard satellite communication infrastructure, including access controls to equipment and control centres). Additionally, a proactive approach involves continuous monitoring and Updates, entailing the regular review and updating of access control policies and mechanisms to adapt to evolving threats and requirements. For instance, Cao, Dang [78] proposed a token-based access control mechanism for smart contracts, which incorporates dynamic adjustment of the access control rules, guaranteeing that only duly authorized users can initiate and execute specific smart contracts. Similarly, de La Beaujardiere, Mital [79] have undertaken a comprehensive examination of the potential applications of blockchain in the context of multi-sensor satellites, contributing to the expanding discourse on integrating advanced technologies to enhance both the security and functionality of space systems.

3.4.4. *Software and firmware security*

State-of-the-art software and firmware security for space communication involve a range of practices, including secure coding, code reviews, and testing to prevent vulnerabilities [80]. These practices are fundamental given the increasing complexity of space systems and the need for high-integrity software [81]. Threat modelling and firmware integrity verification are also crucial to this security approach. However, there is a need for a more integrated approach to security, with security-minded formal verification that combines these analysis techniques [80]. This integrated approach should be incorporated into the software development life cycle, with a focus on building software with security in the context. Nevertheless, it is imperative to acknowledge that these robust security measures may introduce challenges such as compatibility issues, increased payload weight, and elevated power consumption [82].

3.4.5. *Space data encryption and storage*

In space missions, a paramount asset is the data, encompassing mission control processed data, observation requests, distributed data, mission-specific storage, and archived product data. Contemporary utilization of cloud storage facilitates seamless access to a centralized repository, streamlining the distribution and deployment of crucial updates across the satellite system network and associated ground stations. Nonetheless, external commercial providers' cloud systems introduce vulnerabilities and potential failures in their infrastructure, impacting real-time satellite operations and exposing satellite receivers to denial-of-service attacks.

Securing data in satellite communication entails adopting encryption algorithms, such as AES, establishing robust key management systems, implementing secure transmission protocols like SSL/TLS or IPsec, ensuring secure storage mechanisms for data at rest, applying

authentication and access control measures, maintaining physical security, and conducting compliance and auditing activities. For instance, Papoutsis, Howells [83] propose techniques for generating encryption keys based on satellite-specific properties, obviating the need for key storage. Similarly, blockchain emerges as a potential candidate, yet its costly storage space, escalating with the index, prompts consideration of smart contracts as an alternative [78,84].

3.4.6. Vulnerability assessment: identifying and mapping dependencies

Regular vulnerability assessments and penetration testing are imperative to identify and rectify weaknesses in the cybersecurity infrastructure of space missions [85]. These techniques encompass Vulnerability Scanning (scans to identify potential vulnerabilities), Penetration Testing (controlled simulated attacks to unveil security weaknesses), Configuration Review (evaluating configuration settings), Threat Modeling (identifying potential threats and attack vectors), Social Engineering Testing (assessing the human factor through simulated attacks), and Wireless Network Testing (evaluating the security of wireless networks in satellite communication). These methods aid in vulnerability identification, risk assessment, and the implementation of security measures, ensuring protection against potential threats and attacks. Nevertheless, there is a need to integrate automatic vulnerability repair tools to assist smart contract administrators/blockchain transactions in addressing potential vulnerabilities of space missions [78].

3.4.7. Incident response and recovery

In the event of a space mission cyberattack, the swift and effective implementation of incident response and recovery techniques is crucial [86,87]. This encompasses a robust incident response involving the establishment of plans, classification of incidents, containment of impact, and gathering evidence. Effective communication strategies are also crucial, necessitating stakeholders' coordination, active mission control involvement, and engagement with system administrators. The incident response continuum extends to forensic investigation, encompassing the analysis of logs, isolation of systems, and the preservation of critical data. Subsequent to this, the phase of remediation and recovery requires addressing vulnerabilities, patching systems, and enhancing overall security measures. Post-incident analysis becomes integral for organizational learning, policy updates, and the improvement of response processes. Furthermore, to fortify preparedness for future threats, including regular testing procedures is paramount.

3.4.8. Regulatory and policy frameworks

Mitigating cyber threats in space requires technological advancements and practical policy solutions that adapt to evolving threat environments [88]. Existing space security policies, such as Space Policy Directive 5, establish a foundation by incorporating academic research on space cybersecurity [89]. The Tali Manual addresses the legal and liability implications of cyberattacks on space objects, emphasizing the industry's importance of robust cybersecurity measures. Globally, approximately 71 countries possess varying degrees of space capabilities with corresponding frameworks. For example, the Committee on National Security System in the US relies on guidelines to regulate security measures for satellite communications in national security missions [9]. The Australian Space Cyber Framework establishes a common framework for assessing security practices against standards and strengthening the cybersecurity posture of the Australian space ecosystem [90]. In Europe, Germany offers a model for space-industry cybersecurity standards, focusing on the growing cyber threats to the expanding space sector [91]. While the deployment of these frameworks is still in its early stages and faces limitations, their implementation remains necessary to provide an additional layer of protection against cyberattacks.

Nevertheless, the democratization, commercialization, and technological advancements, particularly the ubiquitous connectivity of satellites and associated space infrastructure, have rendered them vulnerable to cyberattacks. These attacks can intercept, corrupt, or control data and systems in space missions for malicious purposes [85]. Since the launch of the first artificial satellite in 1957, the cyber and space domains have become deeply intertwined. Today, operating in one domain inevitably involves interaction with the other. Various organizations have recognized this interdependence, including the North Atlantic Treaty Organization, which designated cyberspace as a "Domain of Operations" in 2016 and extended this designation to space in 2019 [92].

Table 4 outlines the key cyberattack vectors, their descriptions, vulnerabilities, potential consequences, and recommended countermeasures within the context of space systems.

4. Discussions and future directions

The vulnerability of space systems to cyberattacks stems primarily from two factors: 1) the global nature of cyberspace, which creates a platform for borderless attacks, and 2) the imbalance in cyber capabilities within the space domain, making offensive actions more accessible. Drawing on the synthesized findings from previous sections on space cyber-attack methods and mitigation techniques, we see three broad research avenues for improving space mission cybersecurity: 1) technological drivers, focusing on developing and implementing advanced solutions, and 2) regulatory and operational frameworks, aimed at establishing international standards, policies, and 3) fostering collaboration among stakeholders, and the need for a multistakeholder regime.

4.1. Space cybersecurity's technological drivers

The aerospace corporation has identified four significant cyber vulnerabilities in space communication: i) transmission of false data from an untrusted source, ii) giving wrong instruction to manipulate controls (spoofing), the interruption or delay of communication (jamming), and the potential infection of ground-based systems with malware [105]. Consequently, securing connectivity becomes the critical first step, demanding a multi-pronged approach incorporating diverse methods tailored to each vulnerability. IDS/IPS are crucial for space data-flow security but face unique challenges. Limited historical data, constrained data collection, unfamiliar attack patterns lead to high false positive rates, and tight processing power/memory on spacecraft restrict IDS/IPS effectiveness. The AI-enabled algorithm is helpful here, but securing space AI itself is crucial—protecting models and data while staying vigilant against AI-powered attacks like Deep Locker and Malware-GAN [106,107].

Similarly, quantum communication offers robust encryption solutions vital for space cybersecurity [108]. Yet, its deployment faces significant challenges, such as quantum state degradation over long distances and the need for miniaturized hardware engineering to withstand the hostile space environment [12]. Moreover, the brutal space environment with extreme temperatures, radiation, and vibrations threatens satellite components, potentially corrupting data, disrupting communication, and compromising systems [13]. Novel fault-tolerant security mechanisms are crucial to withstand these harsh conditions and ensure mission safety.

Blockchain-based access control in space communication seeks to establish secure and flexible access management through decentralized models and smart contracts. However, further research is required in areas such as dynamic policy enforcement, secure satellite communications, and protocol optimization for resource-constrained space environments [78]. In this context, recent studies have explored the integration of ASCON, a family of lightweight cryptographic algorithms and the new NIST standard for lightweight cryptography, into blockchain architecture [109]. Utilizing a 320-bit permutation for 128-bit security, ASCON has been implemented on various hardware platforms [110]. It offers three variants with distinct block sizes and round configurations. While ASCON focuses on providing lightweight

Table 4
Space cyberattack vectors.

Sub-Attack Vector	Description	Vulnerabilities	Potential Consequences	Potential Countermeasures
Attack vector: Data Tampering [93–95]				
Satellite Communication Interception	Interception and modification of data transmitted between satellites and ground stations	Weak encryption, unsecured communication links, inadequate authentication	Data theft, mission failure, unauthorized access	Strong encryption algorithms (e.g., AES-256), secure communication protocols (e.g., HTTPS, TLS), multi-factor authentication (MFA), Blockchain-Based Integrity checks
In-Orbit Manipulation	RF Interference, Solar Radiation and Cosmic Ray Interference (Cosmic radiation in space induces electronic faults)	Inadequate anomaly detection	Mission failure, data loss, unauthorized control	Tamper-resistant hardware and software, secure boot processes, anomaly detection mechanisms, Post-Quantum Cryptography
Ground Station Compromise	Unauthorized access to ground stations	Weak physical security, network vulnerabilities	Unauthorized access to satellite data, Space mission disruption	Physical security measures (e.g., fences, CCTV, guards), network segmentation, intrusion detection systems (IDS), regular vulnerability assessments
Supply Chain Compromise	Compromised components or software during manufacturing can serve as entry. points for cyber attacks on space systems	Introduction of malware into satellite systems. Long-term system compromise (e.g., hidden backdoors).	Compromised Hardware Lack of Integrity Checks	Blockchain-Enabled Supply Chain Security, AI/ML for Threat Detection Zero-Trust Architecture, Patch Management
Attack vector: Denial-of-Service (DoS) Attacks [96–98]				
Satellite Overloading	Overwhelming a satellite with excessive traffic, causing service disruption	Limited processing capacity, lack of traffic management	Mission failure, data loss, service outages	Traffic filtering, rate limiting, resource allocation optimization, Effective satellite swarming methodologies
Ground Station Disruption	Disrupting the operation of ground stations, preventing communication with satellites	Network vulnerabilities, lack of redundancy	Mission failure, data loss, service outages	Network hardening (e.g., firewalls, intrusion prevention systems), redundancy (e.g., multiple ground stations, backup systems), DDoS protection mechanisms (e.g., cloud-based DDoS mitigation services), Adaptive AI filtering, Quantum key distribution techniques
Satellite Navigation Interference	Jamming or spoofing satellite navigation signals	Vulnerable navigation systems, lack of anti-jamming capabilities	Navigation errors, mission failure	Spread spectrum modulation (e.g., GPS L1C signal), adaptive antenna arrays, anti-jamming techniques (e.g., frequency hopping, time hopping)
Space Debris Collision	Cyber threats redirecting satellites into collision courses with space debris, potentially leading to physical damage	Orbital collision with debris	Mission failure, data loss, service outages	AI-Driven Anomaly Detection, Quantum-Secure Communication, Self-Healing Satellites (Automating system reboots or corrections for minor physical anomalies caused by attacks)
Attack vector: Spoofing [99,100]				
Satellite Signal Spoofing	Transmitting fake satellite signals to deceive ground stations or other satellites	Weak authentication, lack of signal verification	Unauthorized access, mission failure, data loss	Robust authentication mechanisms (e.g., digital certificates, public key infrastructure), time synchronization, anomaly detection (e.g., statistical analysis of signal characteristics)
Ground Station Spoofing	Impersonating ground stations to gain unauthorized access or control	Vulnerable authentication protocols, lack of identity verification	Unauthorized access, mission failure, data loss	Secure communication protocols (e.g., HTTPS, TLS), identity verification (e.g., two-factor authentication, biometrics), access controls
Attack vector: Repudiation [96,101]				
Denial of Involvement	Claiming not to have performed an action	Lack of audit trails, insufficient logging	Legal disputes, loss of trust	Comprehensive logging, non-repudiation protocols (e.g., digital signatures), evidence preservation
False Claims	Making false statements about actions or events	Lack of authentication, weak access controls	Legal disputes, loss of trust	Strong authentication mechanisms, role-based access controls, audit trails
Attack vector: Information Disclosure [41,101,102]				
Unauthorized Access	Gaining access to sensitive information without authorization	Weak access controls, lack of encryption	Data theft, financial loss, reputational damage	Strong access controls, encryption (e.g., AES-256), and data loss prevention (DLP) solutions
Eavesdropping and Signal Interception	Unauthorized access to sensitive data transmitted	Unauthorized access to sensitive data	Data Spying	Robust use of virtual private network
Data Breaches	Unauthorized access to and disclosure of sensitive information	Vulnerable systems, insufficient security measures	Data theft, financial loss, reputational damage	Regular vulnerability assessments, intrusion detection systems, incident response plans.
Attack vector: Elevation of Privilege [101,103,104]				
Exploiting Vulnerabilities	Gaining elevated privileges to access restricted resources	Software vulnerabilities, weak configuration	Unauthorized access, data theft, mission failure	Regular vulnerability scanning, patch management, secure configuration
Social Engineering	Tricking users into revealing credentials or performing unauthorized actions	Phishing, impersonation	Unauthorized access, data theft, mission failure	Security awareness training, phishing simulations, strong password policies

cryptographic solutions for embedded systems, blockchain architecture offers a broader framework for decentralized applications. Together, these technologies, such as a multi-signature and ASCON-based authentication protocol for IoT devices using blockchain [111], can address critical aspects of modern computing: enhancing security in resource-constrained environments and enabling distributed trust in digital transactions.

In the realm of space cybersecurity, ASCON's lightweight yet robust cryptographic properties make it particularly valuable for securing satellite communication networks, protecting ground stations from cyberattacks, and safeguarding space-based IoT networks [112]. By harnessing ASCON's efficiency and cryptographic capabilities, space

missions can safeguard sensitive data, prevent unauthorized access, and significantly bolster the resilience of space infrastructure. Its integration can lead to enhanced data security through encryption and authentication, fortified communication security through the establishment of secure channels and protection against eavesdropping, and strengthened system integrity through secure boot processes and anomaly detection [110,113].

Simultaneously, Zero Trust Architecture offers dynamic security for space systems; challenges like intermittent connectivity, legacy system integration, and limited downlink capacity necessitate customized solutions, including innovative key management for encryption in orbit. This shift from traditional, static security toward user-centric access control requires careful planning for smooth implementation in the unique space environment [114].

Another challenging aspect is updating software on space assets, like satellite firmware, due to remote access limitations and the need for satellite visibility to ground stations, often requiring multiple fly-bys for transmitting updates [13]. Concurrently, software updates can introduce vulnerabilities, highlighting the importance of techniques like software attestation to enhance trustworthiness and mitigate risks associated with flawed updates [115]. A historical example: the Phobos 2 probe inadvertently lost solar lock and communication capabilities due to a faulty software update [116]. Similarly, managing security keys for satellite constellations poses challenges due to the large number of keys needed and the dynamic nature of satellite groups, requiring scalable and efficient key management systems [13]. The anticipated surge in operational satellites, expected to reach approximately 50,000 within a decade [17], will pose unprecedented challenges for operators in managing large-scale satellite constellations, necessitating real-time supervision and management of hundreds or even thousands of satellites to avoid severe consequences from computational or command errors [117,118].

Space cybersecurity relies heavily on space awareness, which involves identifying and tracking operational satellites while monitoring for anomalies and debris, particularly highlighted by events like the 2019 Russian anti-satellite missile test that generated 15,000 pieces of trackable debris [119]. Despite challenges in deciphering intent, advancements like robotic manipulation and telescopes like James Webb promise to enhance observation and safeguard space assets. Similarly, proximity-triggered cyberattacks in SC, particularly those targeting satellites in orbit, require careful consideration. To execute such attacks, the assailant must ascertain the target's location, which is information attainable through local proximity sensors or third-party data [120]. Once they pinpoint the target's location, the attacker can employ their satellite's attitude control and actuators to orient offensive instruments towards the target. Safeguarding against electromagnetic interference and protecting satellite ports during data transfer and servicing missions are vital for ensuring both security and mission success. Nevertheless, space cybersecurity often focuses on system protection, prioritizing data aspects from capture to processing and actively monitoring operations, which is crucial for building robust architectures against evolving threats.

4.2. Regulation and policy framework

While the ITU regulates specific aspects of satellite communications, there is a lack of broader standards and governance in the field [100]. Housen-Couriel argues that the current status quo in practice has resulted in a legal gap, creating ambiguity regarding the applicable international organizations and laws in the context of satellite hacking incidents [4]. For instance, Dual-use space systems, owned commercially but vital for government operations, raise security concerns. Operators may prioritize profit over security, prompting calls for regulations. A specific example of an unresolved issue is encryption in space-based operations, where stakeholders, particularly the service providers, often evade responsibility by arguing it is a matter of consumer choice or merely providing services. Similarly, the debate on the legal rights of satellite operators to defend themselves raises questions. Some suggest granting satellite operators the ability to corrupt files and launch DoS attacks against attackers to regain control, akin to historical maritime practices. However, these "hack-back" rights are controversial [121].

The growing call for the classification of space systems as "critical infrastructure" has been answered by many countries across the globe, such as Australia [122]. However, industry actors have resisted rigid legal standards, contending that status quo requirements are adequate [123]. International regulations hinge on domestic policies, necessitating a holistic approach for national cybersecurity, telecom, and internet governance aligned with global frameworks. Transparency in LEO constellations builds market trust and integrates them seamlessly with global 5G infrastructure. Kulesza and Akcali Gur [18] propose licensing options for LEO satellites considering economic, political, technological, and cybersecurity aspects. For instance, the global space market is valued at $350 billion, with an expected value of $11.1 trillion by 2040 [124]. Likewise, the Australian agency aims to achieve a $AU 12 billion value for the Australian civil space sector by 2030 [20]. Moreover, as of January 03, 2024, approximately 8,377 active satellites are "Orbiting Now" in various Earth orbits [125].

Moreover, the dynamics of power in the space domain are evolving due to the emergence of private companies and new technologies prioritizing commercial opportunities alongside the traditional dominance of established space-faring states. While indications suggest continued dominance by a few states in the near term, it's essential to monitor and analyze these developments to anticipate changes in power dynamics, including cybersecurity implications, amid shifting commercial landscapes and emerging players [26].

While there have been efforts to document and propose communication protocols, the space industry lacks consensus on the optimal approach to implementing secure communications and authentication and determining the appropriate security requirements for different missions [37]. SC lacks KPIs to gauge effectiveness. Implementing standard KPIs and sharing incident reports through dedicated channels like Space System Information Sharing and Analysis Centre (SSISAC) [126] can improve transparency and collaboration. Similarly, regular threat assessments considering evolving technologies, cyber threats, and diverse actors are crucial for developing effective space cybersecurity policies. Incidents like ViaSat KA-SAT network outage highlight the need for proactive measures and assessing the impact of implemented policies.

Space Spectrum policy is vital for space cybersecurity as it allocates dedicated frequency bands, ensures interference-free communication, and regulates spectrum usage to bolster the security and resilience of space systems against cyber threats. Spectrum reuse through integrated sensing and communication offers security benefits but lacks research on seamless integration and legal implications [17]. Similarly, establishing liability frameworks in space cybersecurity is crucial for ensuring accountability and addressing potential damages from cyber incidents. However, existing international space law lacks explicit provisions for cybersecurity, leaving a gap in regulatory frameworks and raising concerns about assigning responsibility and jurisdiction for cyberattacks in outer space [11,127].

The institutional design of space system organizations presents security challenges due to the lack of distinction between IT infrastructure and specialized mission systems, leaving assets vulnerable. To address this, the policy framework should prioritize cybersecurity skill development and comprehensive training programs for personnel involved in space missions to mitigate potential compromises from insider threats and protect sensitive information. Nevertheless, the space missions' policy development and cybersecurity regulatory framework have evolved independently of relevant technical communities, leading to aspirational proposals that may lack actionable steps. Bridging the gap between the policy and technical communities can pave the way for

impactful future work in both fields. Policies should encourage compliance with international space laws, transparency in operations, and developing protocols for de-escalation and collision avoidance while addressing unresolved issues like encryption and promoting sustainable resource use, including debris disposal.

4.3. The need for a multistakeholder international legal regime

In order to effectively cope with the complex and dynamic nature of space cybersecurity, it is essential to establish an inclusive cybersecurity regime that considers the interests of various stakeholders, including corporate, military, scientific, and end-user actors. Such a regime should address technical, economic, social, and political concerns through a pragmatic combination of bottom-up and top-down approaches. A crucial aspect is identifying the key elements requiring protection, such as broadband access, and shaping policy interventions accordingly [11, 128]. Moreover, the approach should be non-hierarchical, ensuring equitable consideration of all stakeholders' concerns. Each participant should be empowered as a valued contributor within the sector, with individual knowledge and expertise. Similar to other aspects of space law and policy, outer space governance in the context of cybersecurity requires clear definitions to address breaches. A balanced approach is necessary, considering the trade-off between protecting space users' privacy and freedom, addressing operational and data accessibility constraints for space service providers and suppliers while safeguarding their business investments, and establishing command and control thresholds for state regulators [129].

5. Conclusion and limitations

While space technology soars to new heights, its vulnerability to cyberattacks casts a long shadow. Existing research, though diverse, often silos technical aspects and neglects the interconnected nature of cyber threats in this unique domain. This study bridges this gap by forging a holistic approach that seamlessly integrates space and cyber domains.

Delving into the unique requirements of SC, the study meticulously examines the vast scope of potential attack vectors, encompassing the ground segment, space segment, user segment, cloud segment, communication channels, and supply chains. It comprehensively outlines counterstrategies and mitigation techniques to fortify the cybersecurity of space missions. On the technical front, research priorities include:

- Specialized intrusion detection and prevention systems tailored to the challenges of the space environment.
- Blockchain-based access control mechanisms for building secure and transparent data-sharing platforms.
- Zero-trust architectures aim to minimize attack surfaces and ensure continuous verification.
- Exploration of quantum technologies to harness their power for enhanced security and threat detection.
- Coordinated defence strategies for satellite constellations, enabling robust protection of interconnected networks.
- Comprehensive space awareness systems enhance situational awareness through comprehensive monitoring and tracking.
- Mitigation of physical satellite attacks by understanding and addressing this unique threat.

Beyond technical solutions, the study emphasizes the necessity of robust regulatory frameworks. It advocates for the establishment of international standards and KPIs for space communication, fostering responsible practices and measuring progress. Key areas for exploration include:

- Developing a highly specialized workforce by nurturing expertise in this critical domain.
- Optimizing space spectrum policy by balancing innovation with security considerations in radio frequency allocation.
- Assessing the economic implications of cyber threats, understanding the financial risks, and potential impact on space operations.
- Establishing norms of behaviour to promote peaceful and responsible activities in the space domain.
- Delineating liability and power dynamics by addressing legal frameworks and navigating challenges in the age of space commercialization.

This study lays a roadmap for securing the future of space exploration. It empowers researchers with new directions, inspires technology developers to innovate, and informs decision-makers to craft a sustainable and resilient Space Cybersecurity framework. By forging a united front against cyber threats, we can ensure space remains a platform for progress, not conflict, for generations to come.

While valuable in summarizing SC research, the review paper has limitations to consider. Focusing solely on English literature risks overlooking key international perspectives. The authors' choices and framing might unconsciously introduce bias, potentially emphasizing specific technical areas over broader legal or international cooperation aspects. Additionally, the review is restricted by the limited availability of data due to classified or unreported space cyberattacks, potentially underestimating the true threat landscape. Furthermore, the absence of quantitative analysis hinders understanding the long-term strategic implications of cyber vulnerabilities.

CRediT authorship contribution statement

Shah Khalid Khan: Writing – review & editing, Writing – original draft, Validation, Project administration, Methodology, Formal analysis, Conceptualization. **Nirajan Shiwakoti:** Supervision, Methodology, Formal analysis. **Abebe Diro:** Writing – review & editing, Investigation. **Alemayehu Molla:** Writing – review & editing, Resources. **Iqbal Gondal:** Supervision. **Matthew Warren:** Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to acknowledge the financial support provided by the Department of Defence Strategic Policy Grants, Australian Government, for this study. The views expressed in this study do not necessarily reflect those of the Department of Defense.

Data availability

No data was used for the research described in the article.

References

[1] D. Livingstone, P. Lewis, Space, the Final Frontier for Cybersecurity? The Royal Institute of International Affairs, Chatham House, 2016.
[2] C. Van Camp, W. Peeters, A world without satellite data as a result of a global cyber-attack, Space Policy 59 (2022) 101458.
[3] Berger, J.F.B., *SpaceX shifts resources to cybersecurity to address Starlink jamming.* https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/, accessed on 07 Jan, 2024, 2022.
[4] J. Pavur, I. Martinovic, Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, J. Cybersecur. 8 (1) (2022) tyac008.

[5] W. Zhijun, Y. Yiming, BD-D1Sec: protocol of security authentication for BeiDou D1 civil navigation message based on certificateless signature, Comput. Secur. 105 (2021) 102251.
[6] M.R. Manesh, N. Kaabouch, Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions, Comput. Secur. 85 (2019) 386–401.
[7] N. Boschetti, N.G. Gordon, G. Falco, Space Cybersecurity Lessons Learned from The ViaSat Cyberattack, ASCEND 2022 (2022) 4380.
[8] S.K. Khan, et al., Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, Accid. Analy. Prevent. 148 (2020) 105837.
[9] M. Manulis, et al., Cyber security in new space: analysis of threats, key enabling technologies and challenges, Int. J. Inform. Secur. 20 (2021) 287–311.
[10] Dunn Cavelty, M. and A. Wenger, *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation.* 2022.
[11] C. Suwijak, S. Li, Global internet access from the low earth orbit: legal issues regarding cybersecurity in outer space, J. East Asia Int. Law 15 (1) (2022) 93–108.
[12] M. Mastriani, S.S. Iyengar, L. Kumar, Satellite quantum communication protocol regardless of the weather, Opt. Quant. Electron. 53 (4) (2021) 181.
[13] V. Varadharajan, N. Suri, Security challenges when space merges with cyberspace, Space Policy (2023) 101600.
[14] A.M. Lubojemski, Satellites and the Security Dilemma, Astropolitics 17 (2) (2019) 127–140.
[15] M. Albakjaji, Cyberspace: The challenge of implementing a global legal framework the impacts of time & space factors, J. Legal Ethic. Regul. Isses 23 (2020) 1.
[16] P.L. Goethals, M.E. Hunt, A review of scientific research in defensive cyberspace operation tools and technologies, J. Cyber Secur. Technol. 3 (1) (2019) 1–46.
[17] Pingyue Yue, J.A., J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, L. Hanzo, *Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead.* https://arxiv.org/abs/2201.03063, 2023.
[18] Kulesza, J. and B. Akcali Gur, *Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband–an International Law Perspective.* Available at SSRN 4424148.
[19] N.J. Van Eck, L. Waltman, Citation-based clustering of publications using CitNetExplorer and VOSviewer, Scientometrics 111 (2) (2017) 1053–1070.
[20] Agency, A.S., Advancing Space: Australian Civil Space Strategy 2019-2028, Commonw. Austr. (2019) available at: https://www.space.gov.au. accessed on May 1, 2023.
[21] J.A. Bleeker, J. Geiss, M.C. Huber, The century of space science, Springer, 2001.
[22] *STARSHIP FLIGHT TEST.* available at: https://www.spacex.com/, accessed on May 1, 2023.
[23] *NASA - Ion Propulsion.* available at: https://www.nasa.gov/centers/glenn/about/fs21grc.html, accessed on 1 May,2023.
[24] G. Kavallieratos, S. Katsikas, An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space, Int. J. Critic. Infrastruct. Protect> (2023) 100640.
[25] B. Lin, W. Henry, R. Dill, Defending Small Satellites from Malicious Cybersecurity Threats, in: International Conference on Cyber Warfare and Security 17, 2022, pp. 479–488.
[26] S. Rementeria, Power dynamics in the age of space commercialisation, Space Policy 60 (2022) 101472.
[27] Yue, P., et al., *On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends.* arXiv preprint arXiv:.03063, 2022.
[28] M. Kirshner, Model-based systems engineering cybersecurity for space systems, Aerospace 10 (2) (2023) 116.
[29] S. Shahzad, L. Qiao, Need for a cyber resilience framework for critical space infrastructure, in: International Conference on Cyber Warfare and Security 17, 2022, pp. 404–412.
[30] *Satellite Security in New Space.* https://airpower.airforce.gov.au/blog/BP27207741; Accessed 04 May, 2023.
[31] E. Ukhanova, Cybersecurity and cyber defence strategies of Japan, SHS Web Conferen. 134 (2022) 00159.
[32] C. Fleming, M. Reith, W. Henry, Securing commercial satellites for military operations: a cybersecurity supply chain framework, Int. Conferen. Cyber Warf. Secur. 18 (1) (2023) 85–92.
[33] S. Kang, D. Qiaozhong, Z. WeiQiang, Space information security and cyberspace defense technology, in: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013, pp. 1509–1511.
[34] J. Lachal, et al., Metasynthesis: an original method to synthesize qualitative literature in psychiatry, Front. Psychiatry 8 (2017) 269.
[35] D. Walsh, S. Downe, Meta-synthesis method for qualitative research: a literature review, J. Adv. Nurs. 50 (2) (2005) 204–211.
[36] Genta, G. *The ground segment.* 2017.
[37] Varadharajan, V. and N. Suri, *Security challenges when space merges with cyberspace.* arXiv preprint arXiv:.10798, 2022.
[38] China-based hacking campaign is said to have breached satellite, defense companies, CNBC, 2023. https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html. Accessed 2 May.
[39] Martin, P.K., et al., *Nasa cybersecurity: An examination of the agency's information security.* 2012. 29.
[40] J. Bardin, Satellite cyber attack search and destroy. Computer and Information Security Handbook, Elsevier, 2013, pp. 1173–1181.
[41] S. Zatti, The protection of space missions: threats and cyber threats, in: Information Systems Security: 13th International Conference, ICISS 2017, Springer, Mumbai, India, 2017. *December 16-20, 2017, Proceedings 13*.
[42] V.L. Pisacane, Fundamentals of space systems, Johns Hopkins University Appli, 2005.
[43] A.J. Gerber Jr, D.M. Tralli, S.N. Bajpai, *Medium Earth Orbit (MEO) as an operational observation venue for NOAA's post GOES-R environmental satellites.* in *Enabling Sensor and Platform Technologies for Spaceborne Remote Sensing*, SPIE, 2005.
[44] K. Thangavel, et al., Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity, in: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), 2022, pp. 1–10.
[45] Economic, U.-C. and S.R. Commission, in: Report to Congress of the US-China Economic and Security Review Commission, US-China Economic and Security Review Commission, 2019.
[46] J. Fritz, Satellite hacking: A guide for the perplexed, Culture Mandala 10 (1) (2013) 5906.
[47] U.S, W.H., *National Space Policy.* https://fas.org/irp/offdocs/nspd/space.pdf. Accessed 04 May 2023, Aug 2006.
[48] Santamarta, R., *A Wake-up Call for SATCOM Security. Technical White Paper.* https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf. Accessed 04 May 2023, 2014.
[49] T.E. Humphreys, et al., Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in: Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), 2008, pp. 2314–2325.
[50] S. Peterson, *Iran Hijacked US Drone, Says Iranian Engineer,*. https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer#:~:text=%22The%20GPS%20navigation%20is%20the,force%20the%20bird%20into%20autopilot. Accessed 4 May, 2023, 15 Dec. 2011.
[51] C. Sacchi, C. Stallo, T. Rossi, Space and frequency multiplexing for MM-wave multi-gigabit point-to-point transmission links, in: 2013 IEEE Aerospace Conference, IEEE, 2013.
[52] Civas, M. and O.B. Akan, *Terahertz wireless communications in space.* arXiv preprint arXiv:2110.00781, 2021.
[53] S.K. Khan, et al., Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks, in: 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), IEEE, 2021.
[54] S. Parkinson, et al., Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE Transact. Intellig. Transport. Syst. 18 (11) (2017) 2898–2915.
[55] V. Linkov, et al., Human factors in the cybersecurity of autonomous vehicles: trends in current research, Front. Psychol. 10 (2019) 995.
[56] Y. Li, et al., Influence of cyber-attacks on longitudinal safety of connected and automated vehicles, Accid. Analys. Prevent. 121 (2018) 148–156.
[57] Q. He, X. Meng, R. Qu, *Survey on cyber security of CAV.* in *2017 Forum on Cooperative Positioning and Service (CPGPS)*, IEEE, 2017.
[58] W. Choi, et al., Voltageids: Low-level communication characteristics for automotive intrusion detection system, IEEE Transact. Inform. Forens. 13 (8) (2018) 2114–2129.
[59] J. Liu, et al., In-vehicle network attacks and countermeasures: challenges and future directions, IEEE Netw. 31 (5) (2017) 50–58.
[60] Colton, K. and B. Klofas, *Supporting the flock: building a ground station network for autonomy and reliability.* 2016.
[61] A. Tepe, G. Yilmaz, A survey on cloud computing technology and its application to satellite ground systems, in: 2013 6th International Conference on Recent Advances in Space Technologies (RAST), 2013, pp. 477–481.
[62] *Fleet Space Technologies: Fleet Portal.* https://www.fleet.space/; Accessed 04 May 2023.
[63] N. Antoni, et al., Re-affirming Europe's ambitions in space: Past, present and future perspectives, Acta Astronaut. 151 (2018) 772–778.
[64] *Google cloud networking incident.* https://status.cloud.google.com//incident/cloud-networking/19020; Accessed 04 May, 2023.
[65] Nichols, S., *AWS's S3 outage.* https://www.theregister.co.uk/2017/03/01/aws_s3_outage/. Accessed 04 May, 2023.
[66] Pavur, J. and I. Martinovic, *Sok: Building a launchpad for impactful satellite cybersecurity research.* arXiv preprint arXiv:.10872, 2020.
[67] S.K. Khan, et al., Cybersecurity regulatory challenges for connected and automated vehicles–State-of-the-art and future directions, Transp. policy 143 (2023) 58–71.
[68] D. Craigen, N. Diakun-Thibault, R. Purse, Defining cybersecurity, Technol. Innov. Managem. Rev. 4 (10) (2014).
[69] Cunningham, D.E., G. Palavincini Jr, and J. Romero-Mariona, *Towards effective cybersecurity for modular, open architecture satellite systems.* 2016.
[70] Forester, C., *Russia" Eavesdropping" on Satellite Operations.* Inside Satellite TV, 2015.
[71] K. Bhasin, J.L. Hayden, Space Internet architectures and technologies for NASA enterprises, Int. J. Satell. Commun. 20 (5) (2002) 311–332.
[72] P. Tedeschi, S. Sciancalepore, R. Di Pietro, Satellite-based communications security: A survey of threats, solutions, and research challenges, Comput. Netw. 216 (2022) 109246.
[73] M.H. Abdulmonem, A.K. Ismail, H. Mostafa, Design and Implementation of Authenticated Encryption Co-Processors for Satellite Hardware Security, in: 2021 International Conference on Microelectronics (ICM), IEEE, 2021.

[74] L. Cazorla, C. Alcaraz, J. Lopez, A three-stage analysis of IDS for critical infrastructures, Comput. Secur. 55 (2015) 235–250.
[75] J.P. Thebarge, W. Henry, G. Falco, Developing Scenarios Supporting Space-based IDS. ASCEND 2022, 2022, p. 4219.
[76] A. Diro, et al., Anomaly detection for space information networks: a survey of challenges, techniques, and future directions, Comput. Secur. (2024) 103705.
[77] R.H.K. Al-Rubaye, A.K. Türkben, Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks, Babyl. J. Netw. 2024 (2024) 45–56.
[78] S. Cao, et al., A blockchain-based access control and intrusion detection framework for satellite communication systems, Comput. Commun. 172 (2021) 216–225.
[79] J. de La Beaujardiere, R. Mital, R. Mital, Blockchain application within a multi-sensor satellite architecture, in: IGARSS 2019-2019 IEEE International Geoscience and Remote Sensing Symposium, IEEE, 2019.
[80] C. Maple, et al., Security-minded verification of space systems, in: 2020 IEEE Aerospace Conference, IEEE, 2020.
[81] M. Klicker, H. Putzer, Toward software-based safety systems in space, in: Proceedings of 5th International Conference on Recent Advances in Space Technologies-RAST2011, IEEE, 2011.
[82] F. Bergamasco, R. Cassar, R. Popova, Cybersecurity: key legal considerations for the aviation and space sectors, Kluwer Law International BV, 2020.
[83] E. Papoutsis, et al., Key generation for secure inter-satellite communication, in: Second NASA/ESA Conference on Adaptive Hardware and Systems (AHS2007), IEEE, 2007.
[84] Y. Zhang, et al., Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage, IEEE Transact. Cloud Comput. 9 (4) (2019) 1335–1348.
[85] J. Pavur, I. Martinovic, The cyber-ASAT: on the impact of cyber weapons in outer space, in: 2019 11th International Conference on Cyber Conflict (CyCon), IEEE, 2019.
[86] S. Madry, Space Systems for Disaster Warning, Response, and Recovery, Springer, 2015.
[87] Hale, B.L., *Mission assurance: a review of continuity of operations guidance for application to cyber incident mission impact assessment (CIMIA)*. 2010.
[88] M.A. Carlo, P. Breda, Impact of space systems capabilities and their role as critical infrastructure, Int. J. Critic. Infrastruct. Protect. 45 (2024) 100680.
[89] DEFENSE, N.S., *Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems*. https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/, accessed on June 6, 2023, 2020.
[90] Australian Space Cyber Framework, ASCF, 2023. https://www.cyberops.com.au/space-cyber-framework. accessed on June 12, 2023.
[91] Govt, G., *Germany Offers Model for Space-Industry Cybersecurity Standards*. https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604, accesed on June 12, 2023, 2022.
[92] Carlo, A., *The Space-Cyber Nexus: Ensuring the Resilience, Security and Defence of Critical Infrastructure*. 2024.
[93] S. Taburoğlu, A survey on anomaly detection and diagnosis problem in the space system operation, J. Intell. Syst.: Theory Applic. 2 (1) (2019) 13–17.
[94] R.M. McGraw, et al., Cyber threat impact assessment and analysis for space vehicle architectures. Sensors and Systems for Space Applications VII, SPIE, 2014.
[95] G. Falco, A. Viswanathan, A. Santangelo, Cubesat security attack tree analysis, in: 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT), IEEE, 2021.
[96] U.-E. Botezatu, Attempted cyber security of systems and operations in outer space: an overview of space-based vulnerabilities, Roman. Cyber Secur. J. 5 (1) (2023) 67–76.
[97] M. Usman, et al., Mitigating distributed denial of service attacks in satellite networks, Transact. Emerg. Telecommun. Technolog. 31 (6) (2020) e3936.
[98] Lane, D., et al., *High-assurance cyber space systems for small satellite mission integrity*. 2017.
[99] B. Cyr, et al., Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing, SpaceSec (2023).
[100] G. Falco, Cybersecurity principles for space systems, J. Aerosp. Inform. Syst. 16 (2) (2019) 61–70.
[101] A. Diro, et al., Anomaly detection for space information networks: A survey of challenges, techniques, and future directions, Comput. Secur. 139 (2024) 103705.
[102] K. Thangavel, et al., Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity, in: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), IEEE, 2022.
[103] E. Ear, et al., Characterizing cyber attacks against space systems with missing data: Framework and case study, in: 2023 IEEE Conference on Communications and Network Security (CNS), IEEE, 2023.
[104] U.I. Atmaca, C. Maple, G. Epiphaniou, Challenges in threat modelling of new space systems: A teleoperation use-case, Adv. Space Res. 70 (8) (2022) 2208–2226.
[105] Corporation, T.A., *CYBERSECURITY PROTECTIONS FOR SPACECRAFT: A THREAT BASED APPROACH*. https://aerospace.org/paper/cybersecurity-protections-spacecraft-threat-based-approach, accessed June 6, 2023, 2022.
[106] D. Kirat, J. Jang, M. Stoecklin, Deeplocker–concealing targeted attacks with ai locksmithing, Blackhat USA 1 (2018) 1–29.
[107] M. Rigaki, S. Garcia, *Bringing a GAN to a knife-fight: Adapting malware communication to avoid detection*. in *2018 IEEE Security and Privacy Workshops (SPW)*, IEEE, 2018.
[108] V. Hassija, et al., Forthcoming applications of quantum computing: peeking into the future, IET Quant. Commun. 1 (2) (2020) 35–41.
[109] I. Elsadek, E.Y. Tawfik, Efficient Programable Architecture for LWC NIST FIPS Standard ASCON, in: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2024.
[110] Kaur, J., et al., *A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard*. arXiv preprint arXiv:2304.06222, 2023.
[111] D Cunha, T.B., *PUF, Multi-Signature and Ascon Based Authentication Protocol for IOT Devices Using Blockchain*. 2024.
[112] S. Dhar, et al., Securing IoT devices: A novel approach using blockchain and quantum cryptography, IoT 25 (2024) 101019.
[113] H. Gross, et al., Suit up!–made-to-measure hardware implementations of ASCON, in: 2015 Euromicro Conference on Digital System Design, , IEEE, 2015.
[114] V. Stafford, Zero trust architecture, NIST Spec. Public. 800 (2020) 207.
[115] B. Min, et al., Antivirus security: naked during updates, Softw.: Pract. Exper. 44 (10) (2014) 1201–1222.
[116] E.V. Bell, *Phobos project information*. https://nssdc.gsfc.nasa.gov/planetary/phobos.html, accessed on 22 Jan, 2024.
[117] I. Del Portillo, B.G. Cameron, E.F. Crawley, A technical comparison of three low earth orbit satellite constellation systems to provide global broadband, Acta Astronaut. 159 (2019) 123–135.
[118] L. Franck, G. Maral, Routing in networks of intersatellite links, IEEE Transact. Aerosp. Electron. Syst. 38 (3) (2002) 902–917.
[119] REUTERS, *Russian anti-satellite missile test endangers space station crew - NASA*. https://www.reuters.com/world/us-military-reports-debris-generating-event-outer-space-2021-11-15/, accessed on 22 Jan, 2024, 2021.
[120] G. Falco, When satellites attack: Satellite-to-satellite cyber attack, defense and resilience, ASCEND 2020 (2020) 4014.
[121] J.D. Rendleman, R. Ryals, Cyber operations to defend space systems?, in: AIAA SPACE 2013 Conference and Exposition, 2013.
[122] Aus_Govt, *Australian Cyber Security Strategy*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf, Accessed on Jan 19, 2023, 2023.
[123] CSRIC, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report,*. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf, Accessed on Jan 18, 2024, Mar. 2015.
[124] CNBC, *Space industry is on its way to $1 trillion in revenue by 2040*. https://www.cnbc.com/2022/05/21/space-industry-is-on-its-way-to-1-trillion-in-revenue-by-2040-citi.html, Accessed 2 May, 2023.
[125] Now, O., *How Many Satellites are in Space?* https://nanoavionics.com/blog/how-many-satellites-are-in-space/#:~:text=As%20of%20January%203rd%202024,satellites%20in%20various%20Earth%20orbits. accessed On 25 Jan, 2024.
[126] ISAC, *SPACE ISAC MISSION*. https://s-isac.org/about-us/, accessed on June 12, 2023, 2023.
[127] F. von der Dunk, Handbook of space law, Edward Elgar Publishing, 2015.
[128] Khan, S.K., N. Shiwakoti, and P. Stasinopoulos, *A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles*. Accident Analysis & Prevention, 2022. 165: p. 106515.
[129] S.K. Khan, et al., Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles, in: Australasian Transport Research Forum, ATRF 2021-Proceedings, 2021. https://australasiantransportresearchforum.org.au/wp-content/uploads/2022/05/ATRF2021_Resubmission_124-1.pdf. Editor.

Shah Khalid Khan is a Postdoctoral Research Fellow at RMIT University's Centre for Cyber Security Research and Innovation, specialising in system-level cybersecurity for complex Cyber-Physical Systems and IoTs. His research assesses the interplay among cybersecurity's technical aspects, regulations, and human factors. He has received prestigious awards, including the "Young Researcher David Willis Award" and the "Austraffic Worldwide Learning Opportunity Award." He is a prolific and passionate cybersecurity researcher, having authored and co-authored over 44 journal papers and conference papers. Prior to his academic career, Shah spent eight years in the information and communication industry, advancing from a field engineer to a team leader through extensive knowledge and experience in communication networks and intelligent data analysis.

A. Professor Nirajan Shiwakoti is an associate professor at RMIT University, specialising in sustainable transport and logistics systems. He is also the program director of the Sustainable Systems Engineering Program at RMIT. He is a key founding member of the Cyber-Physical and Autonomous Systems (CPAS) research group at RMIT and leads the Intelligent Transport and Mobility Systems research theme at CPAS. He has over 180 publications in this field.

Dr **Abebe Diro** is a lecturer at RMIT University's School of Accounting, Information Systems and Supply Chain. He is a cyber security scientist interested in machine learning-based cyber security, and cryptography. He has made outstanding contributions to these fields with publications in high quality journals. The research outputs include pioneering work on distributed machine learning for intrusion detection in Internet of Things. Further, Dr Diro has proven his ability to establish relevant research collaborations with industry through various projects, which is supported by RMIT University's emphasis on aligning research with areas of national interest. He has also established collaborations with academics in Europe, Australia, South Korea, Indonesia and Turkey, where has co-published journal articles with researchers. His high-quality research in cyber security

and his extensive research networks in cyber security and cryptography mark him as a leading researcher at RMIT.

Professor Alemayehu Molla is the Director of the Doctoral Training Centre and leader of the Disruptive Technology and Smart Mobility research cluster at RMIT University Melbourne, Australia.

Professor **Gondal** is Associate Dean, Cloud, Systems & Security at the School of Engineering, RMIT University Melbourne, Australia. He is passionate about translation research in Cybersecurity, Malware analysis, threat intelligence, Blockchain, remote condition monitoring, mobile and sensor networks areas.

Professor Matthew Warren is an experienced and proven cybersecurity and academic leader. He is the Director of the RMIT University Centre for Cyber Security Research and Innovation (RMIT CCSRI) and was formally the Deputy Director of the Deakin University Centre for Cyber Security Research. He is a prolific and passionate cyber security researcher and has authored and co-authored over 300 books, book chapters, journal papers, and conference papers. He is the recipient of the 'Cyber Security Researcher of the Year Award' from AISA in 2020 and a recipient of an ACS Presidents award for his Cyber Security contribution.