International Journal of Critical Infrastructure Protection 43 (2023) 100640

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

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

An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space

Georgios Kavallieratos [*], Sokratis Katsikas

Norwegian University of Science and Technology, Department of Information Security and Communications Technology, Teknologivegen 22, Gjøvik, 2815, Norway

ARTICLE INFO

Keywords:
Space infrastructure
Cybersecurity
Satellites
Literature review

ABSTRACT

Nowadays, assets in space are vital for the provision of critical societal functions such as transportation, communication, production and supply of food, agriculture, etc. The increasing adoption of services provided by assets in space in our every day life, as well as the high dependence on cyberphysical systems, the increased interconnection and the commercialization of space increase the attack surface and poses significant cybersecurity risks to the space infrastructure; several cybersecurity incidents have already threatened assets in space. This work systematically reviews existing studies on the cybersecurity of the space infrastructure, analyzes the main results of each work, organizes and systematizes the current knowledge in the field, and proposes future research directions towards improving the cybersecurity posture of assets in space.

1. Introduction

In 1958, the then US Senator Lyndon Johnson mentioned that controlling space infrastructures will mean controlling the world [1]. Nowadays, the digital transformation increases the reliance of societal critical functions such as transportation of people, food, and products; manufacturing; energy and water management; on space assets and systems. Further, critical infrastructures such as the communication infrastructure highly depend on both ground and space assets [2], while research and innovation leverages space assets to promote knowledge and technology [3]. Additionally, the adoption of satellites in cloud computing communications is increasing, as is also the high number of satellites in earth orbit,[1] due to the significant contribution of the private sector to several space initiatives (e.g., SpaceX, Blue Origin).

Fig. 1 depicts the main segments of the space infrastructure, namely the Space, Link, Ground, and User Segments [5,6]. The Space Segment includes satellites, probes, capsules, space telescopes and space shuttles and provides data to the Ground and User Segments. The Link Segment describes the interconnections of centers, stations and spacecrafts, using ground and space communication links. The Ground Segment consists of the ground-based infrastructure and associated services or support mechanisms and personnel critical to the functioning of the space system, such as satellite monitoring and control, uplink and downlink ground stations and mission operations centers. Last, the Link Segment describes the capabilities that can be hand-held, or mounted on several infrastructures such as communication, maritime vessels, and aircrafts.

The increased dependence on space infrastructure makes the protection of its cybersecurity important; however, several challenges exist towards achieving this. Several cybersecurity incidents have been reported in the literature [7,8]. Such incidents include the disruption of the communication between satellites and subscribers due to a satlink/downlink hijacking attack [9]; GPS jamming and spoofing attacks that targeted maritime GPS receivers [10]. In 2011 adversaries attacked NASA's Jet Propulsion Laboratory (JPL) and gained full control over mission-critical systems [11]. The cybersecurity posture of the space infrastructure, in terms of threats, vulnerabilities, and risks, has not been fully studied. The increasing adoption of COTS systems, the lack of threat modeling for the space infrastructure and the increasing cyber incidents create the need to systematically review existing research with an eye towards finding the appropriate directions for cybersecurity research and solutions for the space infrastructure. Systematic reviews are beneficial for researchers to inform decisions, processes, and conclusions [12].

Motivated by the discussion above, this paper aims to systematically analyze the scientific literature on the cybersecurity of the space infrastructure. To this end, the state of play of cybersecurity in the four segments of the space infrastructure – space, link, ground, and user – is captured in terms of threats, risks, attacks, and controls. Two focus areas are studied, namely the space infrastructure as a whole and satellites in particular. Additionally, legal issues of cybersecurity in space are also examined, and future research directions are proposed.

[*] Corresponding author.
E-mail addresses: georgios.kavallieratos@ntnu.no (G. Kavallieratos), sokratis.katsikas@ntnu.no (S. Katsikas).

[1] On July 20, 2023 there were 8256 objects in orbit [4].

https://doi.org/10.1016/j.ijcip.2023.100640
Received 29 July 2023; Received in revised form 7 October 2023; Accepted 16 November 2023
Available online 23 November 2023

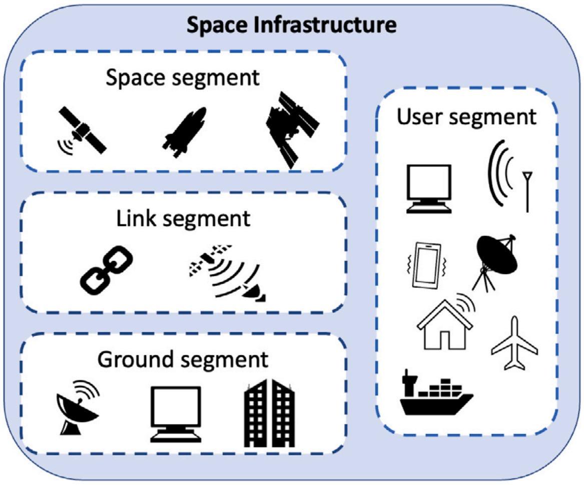


Fig. 1. Space infrastructure structure.

The remainder of this paper is as follows: In Section 2 we discuss earlier surveys of aspects of cybersecurity in the space domain. Section 3 describes the research methodology and Section 4 presents the results of the systematic literature review. In Section 5 the results are discussed and future research directions are proposed. Finally, Section 6 summarizes our conclusions.

2. Related work

Several works in the literature have examined cybersecurity aspects of the space infrastructure. A comprehensive survey of space information networks is conducted in [13], where the security of the physical layer is extensively analyzed to facilitate security by design principles in satellite network designs. A survey of the security issues of routing and anomaly detection in space information networks (SINs) is provided in [14]. The protocols are reviewed considering four aspects, including SINs routing types, single-layer routing, multi-layer routing, and intelligent routing-based machine learning. A survey in sustainable satellite communication is provided in [15], whereby traffic management, debris detection, environmental impacts, spectrum sharing, and cybersecurity aspects are discussed. A state of the art analysis for cybersecurity of space assets focusing on threats, vulnerabilities, and past incidents in the space infrastructure is provided in [16]. However, a systematic method of analysis has not been followed and security aspects such as risks, requirements, and cybersecurity legal issues are not included. A survey on the application of software defined networks in satellites and the accordant research challenges and directions is provided in [17]. A review on the security of the physical layer in satellite communications, providing a comparison between the existing applications along with the security goals towards identifying research gaps and future directions for research is reported in [18]. A survey on secure routing protocols in satellite networks considering different attacks and applications is provided in [19]. Finally, a review of threats, solutions and research challenges in satellite communications is provided in [20].

None of the above studies provides a systematic analysis of the cybersecurity of the space infrastructure. Further, most of these surveys focus on satellite communications and infrastructure only. Cybersecurity aspects of the space ecosystem, including space assets, ground infrastructures, and satellites have only partially been examined.

3. Methodology

Our analysis of the state-of-the-art of the cybersecurity of the space infrastructure is based on a systematic approach that allows for the identification, highlighting, and evaluation of several works that are then analyzed and compared.

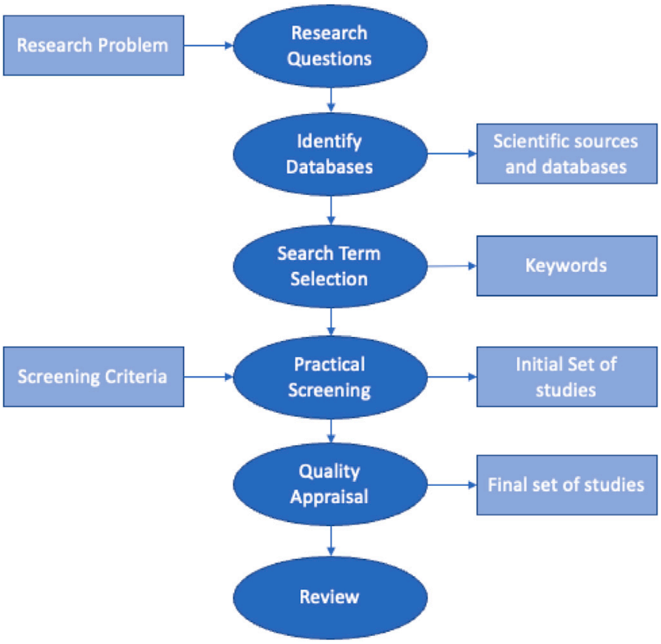


Fig. 2. SLR process flowchart.

The scope of the Systematic Literature Review (SLR) is to carry out exhaustive research on the state of play of cybersecurity in the space infrastructure. Several methods for performing SLRs have been proposed in the literature [21–23]. In this study we follow the steps of the SLR method described in [24,25]. This method is chosen as the most appropriate for this study, as it provides detailed guidelines to review both quantitative and qualitative works [26]. Furthermore, the SLR follows the recommendations of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement [24,27] that it is followed by many SLRs in the literature [28,29]. The method includes the following distinct steps, depicted in Fig. 2 and described in detail in the sequel:

- **Select Research Questions**: The purpose of this literature review is to search for and identify publications on aspects of cybersecurity in the space infrastructure. This review aims at providing a comprehensive analysis of the field in terms of research activities, publications, methods, and trends towards making recommendations for future research. Accordingly, the following research questions were defined:
  - RQ1: What is the current state of the art of the cybersecurity of the overall space infrastructure?
  - RQ2: What is the current state of the art of the cybersecurity of satellites in particular?
- **Select Bibliographic Databases and Sources**: The SLR is performed in the following academic research databases: IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus. These databases have been selected as the most appropriate for this study, according to the recommendations for conducting literature reviews in the field of computer science [30].
- **Search Terms Selection**: The process includes two groups of terms: the first group is related to the targeted infrastructure (space, outer space, orbital infrastructure, satellite, cubesats) and the second to the cybersecurity domain (cybersecurity, cyberattacks, risk, threats, vulnerabilities, countermeasures, mitigation

Table 1
Search strings.

1st group	Terms	2nd group
Space		Cybersecurity
OR		**OR**
Outer space		Cyberattacks
OR	**AND**	**OR**
Orbital Infrastructure		Risk
OR		**OR**
Satellite		Threats
OR		**OR**
Cubesats		Vulnerabilities
		OR
		Countermeasures
		OR
		Mitigation Techniques

techniques). The terms and their combinations are illustrated in Table 1. The search returned 107 sources.

- **Practical Screening**: The following inclusion and exclusion criteria were applied:
  - Only articles that are published in the English language are considered.
  - Duplicate articles are excluded.
  - This study reviewed scientific articles published in conferences, workshops, and journals; and PhD and MSc theses of significant relevance to the examined topic. Presentations, editorials, and posters are excluded.
  - The article must be directly related to cybersecurity of the space infrastructure and/or of satellites.
  - Although cybersecurity issues in the space infrastructure appeared as early as 1960, the proliferation of cyber components in space missions started recently. Whereas most of the incidents before 2010 focused on critical military assets in orbit [1], a wave of jamming incidents started in 2010 [31]. Accordingly, this Systematic Literature Review (SLR) examines the relevant literature since 2010.

  After the screening process, 76 articles were retained.
- **Quality appraisal**: The articles retained after the screening were evaluated in terms of relevance, significance, and impact. The final number of sources to review was 67.
- **Review of articles**: The selected sources were categorized according to the focus area – space infrastructure or satellites – and are subsequently reviewed considering the research questions to produce a summary of the content organized as per the cybersecurity aspects *threats, attacks, risks, countermeasures, vulnerabilities, legal issues, cybersecurity requirements*.

4. Results

Fig. 3 depicts the distribution of the reviewed sources per space segment. The majority of the existing works focus on the link segment and particularly on satellites, while only three and two studies focus on the ground and the user segments respectively. The space segment has been addressed in nineteen out of the reviewed sixty six sources.

Although cybersecurity of space assets is not a new research topic [32], only twenty out of the sixty six reviewed papers were published before 2020. Further, most of the cybersecurity research is conducted in the USA: twenty six out of the sixty six reviewed works are published by USA institutions, eighteen by European, eleven by UK and four from Oceania. Only seven works were published by authors in Asian institutions and organizations.

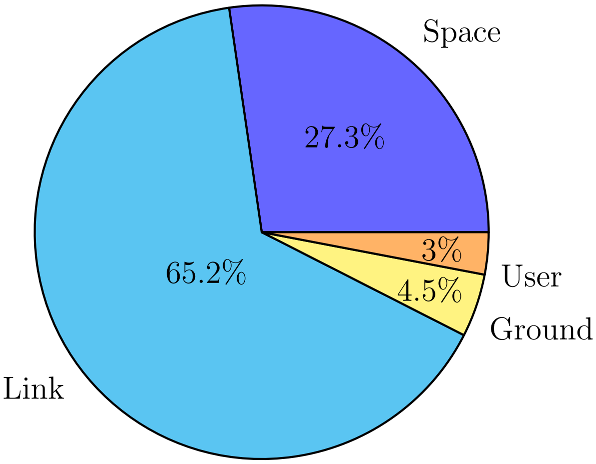


Fig. 3. Reviewed sources per segment.

Most of the research in the last decade is on the cybersecurity of satellites: Nineteen works have studied cybersecurity aspects in the overall space infrastructure and forty seven have focused on satellites. This is possibly due to the fact that satellites are the main components in contemporary communications and facilitate the operations of both national and international critical infrastructures [33]. Nevertheless, many of the papers that focus on satellites include some high-level overview of cybersecurity in the overall space infrastructure. Accordingly, the results of the SLR are presented in two focus areas, one on the overall space infrastructure and one on satellites in particular. The former area comprises systems, components, and interconnections in all four space segments – space, link, ground, and user – whereas the latter focuses on satellite components and communications. Five out of the sixty six studies are reviewed in both the space infrastructure and satellite focus areas of the review, in Sections 4.1 and 4.2 respectively.

The analyzed works explore different cybersecurity aspects, namely *threats, attacks, risks, countermeasures, vulnerabilities, legal issues, cybersecurity requirements*; the analysis follows these classes.

4.1. Space infrastructure

As shown in Fig. 4, nineteen out of the sixty six reviewed articles analyze the cybersecurity of the space infrastructure. The majority of them focus on threats and attacks while only one article discusses risks, requirements, and legal issues.

4.1.1. Threats and attacks

Several cybersecurity threats and attacks against the space infrastructure have been explored in the literature. Fig. 5 presents a proposed taxonomy of these. The threats that have been discussed in the literature are shown in the figure, along with the corresponding references. It can be noticed that the majority of the works focus on the spoofing and jamming threats, while only a few sources discuss more sophisticated attacks and threats such as loss of control and elevation of privileges. Further, most of the sources discuss and analyze general threat categories and attacks; this is possibly because in many cases technical details and experimental platforms are not easily accessible.

Spoofing: The spoofing threat is among the most prominent, since it is described in most of the reviewed works [2,7,32,34–41]. Spoofing has been characterized as being among the most common threats targeting communications in the space infrastructure [40,42,43]. One way for performing a spoofing attack is to compromise a satellite receiver and create fake signals, that appear to be originating from the compromised satellite. Alternatively, an adversary may use a GPS signal simulator or create a software-defined network to perform a false data injection attack and spoof the satellite signal [2]. Cyber threats that target the physical disruption of space assets are presented in [44],

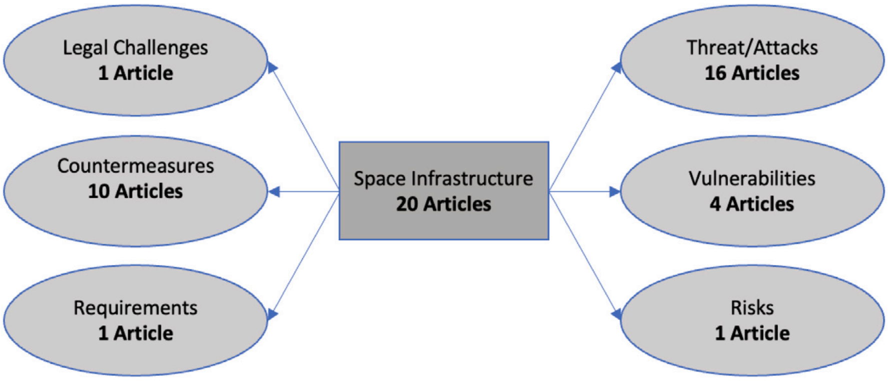


Fig. 4. Cybersecurity aspects addressed in space infrastructure.

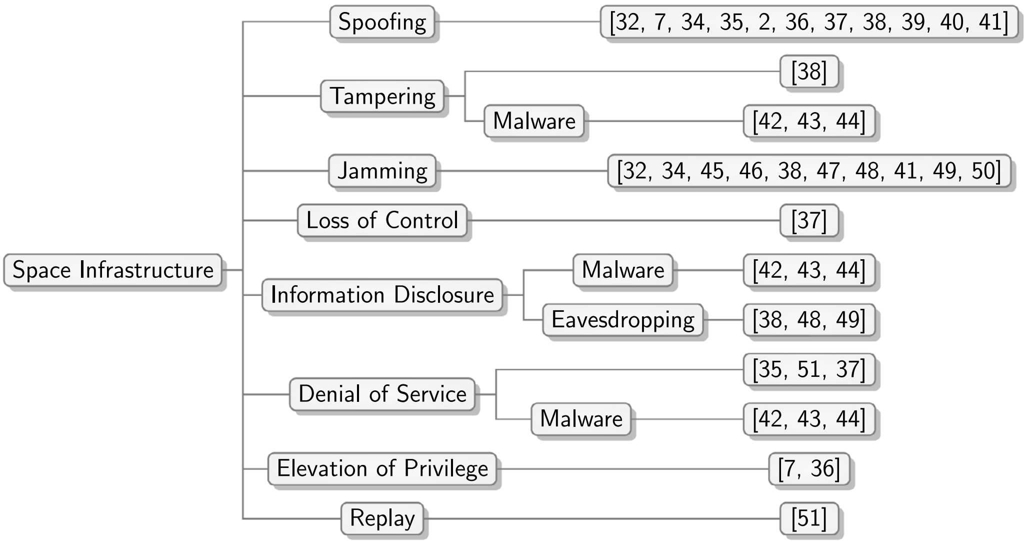


Fig. 5. Space threat taxonomy.

where the analysis focuses on spoofing activities. The cybersecurity posture of the ground, space, and link segments was examined in [39], which focused on the spoofing threat. In [2] a GPS spoofing attack is analyzed; a use case that changed the fixed position of a satellite is included. The spoofing threat in the link segment is characterized as the most critical in [32]. It was identified in [35] among the most critical ones also in the space segment, particularly as regards critical operations. Space mission-specific cyber threats are analyzed in [37] and spoofing was among the most critical threats for navigation missions. Moreover, spoofing is characterized as the most critical threat for NATO's space assets in [45]. The spoofing threat for space assets is analyzed by using the STRIDE methodology in [46]. The threat is also discussed in [38], which analyzed specific attack scenarios such as attacks through faulty or malicious hardware and software components; attack against the links between satellites and ground control stations; attack on terrestrial command and control or data relay stations; attack against the user segment of space systems — terminals or devices receiving satellite signal and closely related; and exploitation of satellite links for hacking other targets. In the link segment, a reconnaissance attack that implemented a spoofing threat by leveraging single sign on vulnerabilities was deployed in an experimental environment [7]. A discussion of spoofing attacks, based on the vulnerabilities of the space and link segments, is provided in [47].

Tampering: The tampering threat has also been discussed in the literature [38,48–50]. Tampering is discussed within the context of several cyberattacks in [38]. Such attacks are attacks against the links between satellites and ground control stations; attacks on terrestrial command and control or data relay stations; attacks against the user segment of space systems — terminals or devices receiving satellite signal and closely related, and exploitation of satellite links for hacking other targets. A tampering attack could change the direction of the satellite's solar panels, directing them towards the sun, thus destroying the batteries and resulting in the satellite to lose power and, eventually, hit the Earth [38]. Both technical and legal aspects of tampering attacks are also discussed in [48], which focuses on the attendant risks and mitigation techniques. A recent tampering cyberattack against the space infrastructure is discussed in [50]. The cyberattack is based on the wiper malware that infected ground segments where the payload control center, hardware components, and embedded software are critical. Further, a unified cybersecurity testbed to analyze tampering threats was proposed in [49].

Jamming: The jamming threat in space infrastructures has been examined in [32,34,38,41–44,46,51]. The cyber threats, including jamming, that target the physical disruption of space assets are presented in [44]. By leveraging the increasing dependence on software-defined networks [52], an adversary may modify the settings of the networks and perform a jamming attack by sending jamming signals on the payloads. Moreover, NASA examined the jamming threat in both institutional and mission related systems [51]. The jamming threat is briefly discussed in [41,43] as one of the most comment threats in space infrastructure. Several threats against the ground segment are discussed in [42], and jamming is found to be among the major ones, as is also in [32]. Jamming cyberattacks that target the communication networks, satellites, and ground stations are discussed in [34]. Jamming in space assets is analyzed in [46] by using the STRIDE methodology, whereas in space operations it is analyzed in [38], where attackers' motivations such as finance, espionage, disruption, politics and retaliation are considered. The jamming threat and its impact on the confidentiality, integrity, and availability attributes in space assets, missions, and communications are examined in [52].

Loss of Control: Space mission-specific cyber threats are analyzed in [37]. The identified threats are deliberate interference and loss of control and viral attack targeting an observation exploration mission. An adversary could seize control of a space asset through a cyber attack (e.g., by gaining administrative access) and disrupt the asset's communication and/or electronics circuits, that may lead to a situation perceived as an accidental malfunction.

Information Disclosure: The information disclosure threat that can materialize through a malware or eavesdropping attack has been discussed in several works [38,43,48–51] and its technical and legal aspects are discussed in [48]. An attacker could compromise a user account and gain access to unauthorized information. In 2018, an account of an external user was compromised and used to steal approximately 500 megabytes of data from a space system [51]. The threat is further discussed in [43,51], where account has been taken of eavesdropping techniques. Different categories of cyberattacks targeting the space infrastructure, such as attacks through faulty or malicious hardware and software components and attack against the links between satellites and ground control stations are discussed in [38]. Additionally, the wiper malware that targeted ground station components was analyzed in [50]. By leveraging a unified cybersecurity testbed for the satellite, aerospace, avionics, and maritime sectors, the impact of information disclosure is discussed in [49].

Denial of Service: Denial of service attacks against the space infrastructure are examined in [35,37,45,48–50]. An attacker may, for example by employing laser dazzling and blinding, create temporary disruptions and generate interference in command and control systems and logistics networks. In 2010, a software update of the GPS Ground Segment caused a denial of service and the impact of this attack was observed on 8,000 to 10,000 military receivers for several days [37]. The denial of service attack that targets the critical operations of the space segment is discussed in [35]. Space mission-specific cyber threats are analyzed in [37] while an overview of the regulatory aspects in the space infrastructure related to denial of service attacks are presented in [48]. The attack is classified among the most critical ones for NATO's space assets in [45]. An analysis of a denial of service attack focusing on the wiper malware is presented in [50].

Elevation of Privilege: The elevation of privilege attack in the ground segment is discussed in [7,36]. When there is a lack of appropriate security controls, an attacker may gain access to critical components and perform unauthorized activities. In 2012, an attacker illegally accessed numerous systems belonging to NASA, the Pentagon, the Romanian government, and U.S. commercial entities [7]. A reconnaissance attack where the adversary aimed to acquire privilege access to the ground base system and exploit vulnerabilities of the single-sign-on technology was deployed in an experimental environment [7]. Space situational awareness is discussed in [36] as a measure to improve cybersecurity against such threats.

Replay: The replay attacks against the space infrastructure are briefly discussed in [45], in relation to NATO's space-based strategic assets. This type of attack is identified as being among the most critical ones for such assets. A replay attack may target the communication between space assets (e.g., satellites and ground stations) and cause damage to the communication links, thus making them unavailable.

4.1.2. *Vulnerabilities*

According to [45], the most critical vulnerabilities of the space assets are back-doors in encryption; the supply-chain security of satellites; lack of authentication in terminals located in ground stations; and data exchange interfaces used between the military and civil sectors. The major vulnerabilities in the space infrastructure in particular are the increased communication between the space assets (e.g., satellite to satellite communication); the continuous adoption of COTS; and the lack of guidelines, standards, and regulations [40]. Among these, COTS components; software-centric assets; wide coverage of satellites; limited in space repair; cascading risks; and third party facilities are among the most critical vulnerabilities in the space infrastructure, according to [43]. A discussion on the vulnerabilities and risks of the space infrastructure with particular focus on the use of AI technology is found in [41], where telemetry; tracking and command; electronics — avionics; and the onboard data handling system are identified as the most vulnerable space assets. Additionally, the use of legacy systems, the adoption of COTS systems, and the increasing interconnectivity of the IoT increase the attack surface.

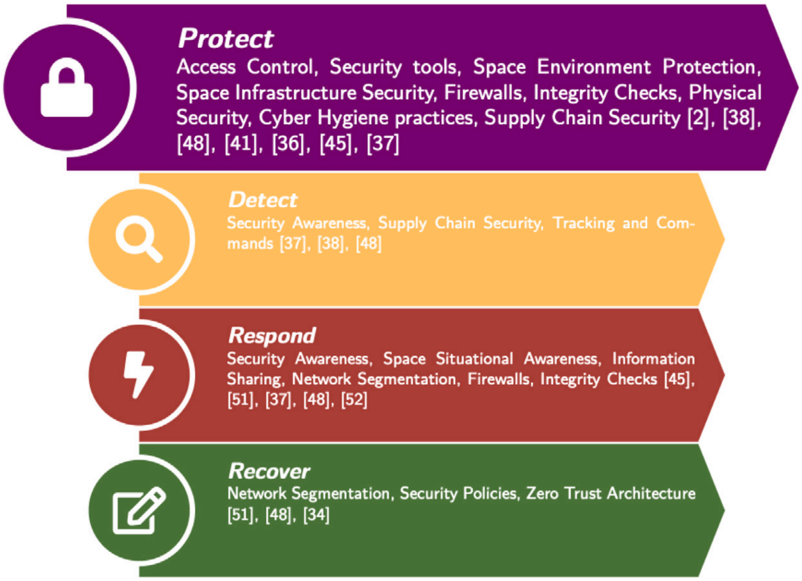
4.1.3. *Risks*

The risk which cyberattacks pose to the space infrastructure is discussed in [53], which also proposes a set of best practices and guidelines, and analyzes existing national and international initiatives for space cybersecurity. Cybersecurity incidents in space systems, aviation, electricity networks, and general space assets (e.g., satellites) are analyzed and attacker profiles are discussed. However, the risks are not systematically assessed.

4.1.4. *Countermeasures*

The mitigation of the risks resulting from the threats, attacks, and vulnerabilities discussed previously has been addressed in the literature by proposing several countermeasures. However, all the proposed measures are techniques of a generic nature and do not focus on specific threats, vulnerabilities, and space assets. Fig. 6 depicts the countermeasures that have been proposed for the space infrastructure; the classification follows the NIST CSF [54] core functions. It can be noticed that most of the identified countermeasures focus on the *protect* function. The *detect* and the *respond* functions include the basic security recommendations for space assets to foster security by design principles and increase the cybersecurity awareness of the personnel. The *recover* function is only partially covered by the recommended countermeasures.

Protect: Several cybersecurity controls have been proposed to protect against cyberattacks in space [2,36–38,41,44,51]. A baseline of security controls to protect space infrastructure is proposed in [2]. These are: access control management, development of security tools, and increase of the security awareness of the personnel in the space infrastructure. Similarly, the basic cybersecurity recommendations for space assets are provided in [38]. These are access control, physical security, cyber hygiene practices, and risk management of the supply chain risks. NASA, in [51], by leveraging the NIST cybersecurity framework, identified the general security controls such as inventory of hardware and software assets; vulnerability assessments; secure configurations; continuous maintenance and patching; malware defenses; data protection; and incident response policies and procedures. Additionally, a baseline of security controls for space assets is also proposed in [36,41], that focus on the encryption of telemetry; tracking and commands; and foster the cyber resilient system by design. The core components to increase the cybersecurity posture of the space infrastructure are space situational awareness, space environment protection and preservation, and space infrastructure security, according to [44]. Furthermore, countermeasures are discussed in [37], where physical, personnel, and information pillars, including the application of firewalls focusing on tele-commands and telemetry; integrity checks; encryption of communications; increasing cybersecurity awareness; and establishment of cybersecurity policies to detect and mitigate cyber risks are considered.



Protect
Access Control, Security tools, Space Environment Protection, Space Infrastructure Security, Firewalls, Integrity Checks, Physical Security, Cyber Hygiene practices, Supply Chain Security [2], [38], [48], [41], [36], [45], [37]

Detect
Security Awareness, Supply Chain Security, Tracking and Commands [37], [38], [48]

Respond
Security Awareness, Space Situational Awareness, Information Sharing, Network Segmentation, Firewalls, Integrity Checks [45], [51], [37], [48], [52]

Recover
Network Segmentation, Security Policies, Zero Trust Architecture [51], [48], [34]

Fig. 6. Countermeasures for the space infrastructure.

Detect: To facilitate the detection of cyberattacks against space assets, security mechanisms such as security awareness and tracking and commands have been proposed [37,38,51]. For attack detection techniques, the establishment of cybersecurity policies to detect and mitigate cyber risks and increase cybersecurity awareness are proposed as controls in [37]. Cybersecurity recommendations for space assets such as supply chain security are provided in [38]. Further, NASA in [51], proposed security controls such as malware defenses.

Respond: Practices such as cybersecurity awareness programs, space situational awareness, information sharing, network segmentation, firewalls, and integrity checks have been proposed as response measures in case of a cyber incident [37,44,45,47,51]. Security countermeasures such as space situational awareness, space environment protection and preservation, and space infrastructure security are discussed in [44]. B. Unal, in [45], provides general recommendations about policies, organizational procedures, and training, with a focus on NATO's infrastructure. Specifically, information sharing, establish of security awareness programs, and network segmentation between military and civilian networks are among the most prominent proposed controls. Furthermore, countermeasures to respond in case of a cyber attack are discussed in [37], which considers physical, personnel, and information pillars, including the application of firewalls focusing on tele-commands and telemetry; integrity checks; encryption of communications; and increasing cybersecurity awareness. Malware defenses and incident response policies and procedures were proposed in [51]. Further, cybersecurity recommendations for space infrastructures focusing on emerging technology (e.g., quantum computing) and policy making to support incident response in space are discussed in [47].

Recover: The recovery function of the NIST framework is only partially addressed in [34,45,51], where a set of cybersecurity guidelines to ensure recovery in case of a cyber attack and policy development are proposed. Similarly to the discussion on controls in the *Respond* function, B. Unal, in [45], provides general recommendations about policies, organizational procedures, and training, with a focus on NATO's infrastructure. NASA, in [51], by leveraging the NIST cybersecurity framework, identified generic security controls such as inventory of hardware and software assets, vulnerability assessments, secure configurations, continuous maintenance and patching, malware defenses, data protection, and incident response policies and procedures. A baseline of recommendations focusing on business continuity and recovery policies development and risk management procedures for space assets is provided in [34].

4.1.5. Requirements

The specification of cybersecurity requirements facilitates the development both of secure space assets and of cybersecurity standards and guidelines. Only one source was found that discusses such requirements: Ref. [37]. The suggested requirements focus on tele-commands (ground to space), telemetry (space to ground), and payload data (space to ground networks). The availability, integrity, authentication, confidentiality, and sequencing (anti-replay) requirements are identified as the most critical ones for space assets.

4.1.6. Legal issues

L. Palmqvist et al. in [40] provide a general overview of the current legal issues of cybersecurity in the space infrastructure. The legislation about space and cybersecurity in Sweden is extensively discussed, and the lack of the necessary cybersecurity aspects in space regulations is highlighted. Neither the international laws nor the space-specific laws comprehensively cover cybersecurity in space. Even though general reference to international laws and regulations relevant to the cybersecurity of the overall space infrastructure is made in several publications [55–57], these sources focus on legal issues pertinent to satellites and are therefore reviewed in the appropriate subsequent Section 4.2.6.

4.2. Cybersecurity of satellites

The cybersecurity of satellites has been extensively, compared to the space infrastructure, analyzed in the literature. As it can be seen in Fig. 7, forty seven articles out of the reviewed sixty six focus on the cybersecurity of satellites.

4.2.1. Threats and attacks

Fig. 8 depicts the threats against satellites as proposed in the reviewed sources. The spoofing, jamming, and denial of service attacks have been analyzed the most in the scientific literature. Similarly to the space infrastructure, malware and eavesdropping techniques have been leveraged for tampering, information disclosure, and denial of service attacks. Although the level of detail of the identified threats is similar to that for the space infrastructure, attacks and threats against satellites have been analyzed more thoroughly. The accessibility of the relevant infrastructure, its connectivity, and the dependence of several critical sectors, such as power grids, maritime, and supply chain, on it are among the main reasons for this difference.

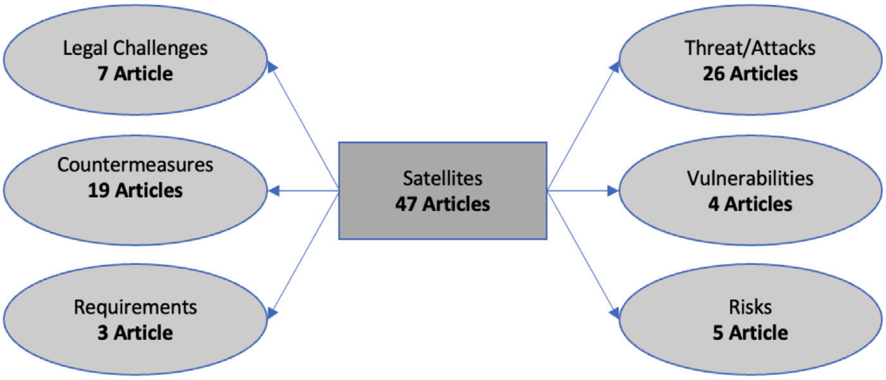


Fig. 7. Cybersecurity aspects addressed in satellites.

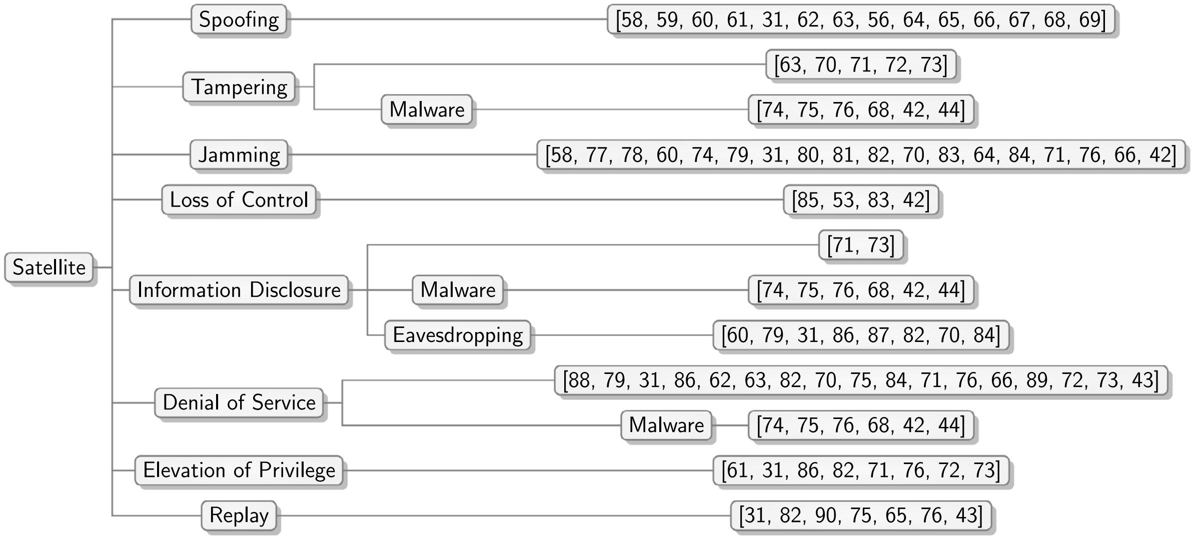


Fig. 8. Taxonomy of threats against satellites.

Spoofing: Several works in the literature discussed the spoofing threat in satellites [31,56,58–69]. Spoofing may aim to capture, alter, and re-transmit a communication signal so as to mislead the recipient to accept it as originating from the intended sender. Attacking satellites via spoofing involves taking over a space communication infrastructure by masquerading as an authorized user and sending false commands causing the spacecraft to malfunction or to fail its mission. The MATRIX and the STPA-Sec approaches are leveraged to explore spoofing threats in satellite systems in [59]. The spoofing threat is among the most common threats to satellites, as it may result in collisions and communication disruptions according to [68,69]. The potential impact of spoofing threats in the four space segments of satellites is discussed in [66]. The spoofing threat is among the most critical according to [67], as it may result in satellite shutdowns and financial damages. An overview of security incidents in satellite infrastructures is provided in [31], and spoofing is identified as being among the most critical threats. The most critical spoofing attacks against satellites are identified in [58], where the focus is on loss of control, pre-launch supply chain attacks, and post-launch supply chain attacks. The major security threats on the operational, communication, and supply chain environments of small satellites are analyzed in [61] and spoofing is among the most critical ones. Past incidents in the space sector and the cybersecurity perspectives, including spoofing attacks on the space, user, and ground segments of small satellites are analyzed in [60]. The spoofing threat is discussed and analyzed in the context of past cyber incidents also in [62,63]; by leveraging the attack trees methodology three cyberattacks against the CubeSat infrastructure are analyzed. The cybersecurity needs of the European space infrastructure are analyzed in [64] taking also into consideration spoofing threats.

Tampering: Several works in the literature have discussed the Tampering threat in satellites [48,50,63,68,70–76]. An adversary is able to add, delete, or otherwise modify files by gaining unauthorized access to the satellite systems. This can lead to the misdirection of the satellite or to disruption of the communication with the ground segment [73]. Further, the tampering threat is analyzed in [75] considering the space, ground, link, and user segments. The potential threats that target small satellites are presented in [74]. The space assets, attack motivations, and attacker profiles are analyzed and the STRIDE method is utilized in [71], where an interception of data attack in satellites is analyzed. A security analysis of cubesats is provided in [63]; by leveraging the attack trees methodology three cyberattacks against the cubesat infrastructure, namely denial of service, data tampering, and disabling cubesat communications are analyzed. A small satellite vehicle was analyzed in [70] by leveraging the NIST cybersecurity framework, and data tampering is identified as being among the most critical threats. The cybersecurity challenges of satellite networks are presented in [48], where the malware threat is analyzed. Tampering is characterized as one of the most critical threats in small satellites in [72], by leveraging the attack trees methodology. Similarly, the cybersecurity threats of satellites are identified in [73] by utilizing the STRIDE and DREAD methods, and Tampering is identified as being among the most critical ones. The criticality of tampering threat is also discussed in [76]. Additionally, the ViaSat cyberattack, in which the malware wiper targeted the ground segment to disrupt the communications of the satellite infrastructure is analyzed in [68].

Jamming: The jamming threat is among the most common and critical ones for satellites [31,48,58,60,64,66,70,71,74,76–84]. The jamming attack could affect the normal operation of a satellite by disrupting the radio communication used by satellites to receive commands [78]. The jamming threat is discussed in [81] and has been analyzed considering several malicious actors in space such as nation-state, professional or amateur hackers, organized criminals, and insiders. A jamming threat that targets the communication links between ground and space segments in the context of satellites is analyzed in [74]. The jamming threat in a small satellite system is analyzed by leveraging the NIST cybersecurity framework in [70]. Furthermore, the jamming threat is analyzed by considering kinetic, non-kinetic, electronic, and cyber attacks in [83]. The jamming threat in Galileo, Copernicus, and mega-constellations and cubesats is analyzed considering several cyber incidents in [64]. Software-defined spoofers are characterized as one of the most critical techniques to perform GPS jamming [78]. By leveraging the STRIDE methodology, the jamming threat is analyzed along with the attack motivations and attacker profiles in [71]. Additionally, a taxonomy of threats against satellites, that includes threat agents, targets, actions, and consequences, is proposed in [79]. The jamming threat is analyzed by considering the aforementioned taxonomy and has been characterized as being among the most critical ones. Moreover, past incidents and the cybersecurity perspectives of the space, user, and ground segments of satellites are analyzed in [60] and the jamming threat is among the most critical and well-known ones. The main threats for small satellites are identified in [58] where loss of control, pre-launch supply chain attacks, and post-launch supply chain attacks are among the most critical ones. The jamming threat and its effects on the on-orbit space infrastructure are analyzed in [77]. Further, the main cyber incidents in space systems, particularly in satellites, are analyzed and the existing technical and organizational challenges are presented in [78]; the main threats identified are cyber-espionage, GPS jamming, and GPS spoofing. The criticality of the jamming threat in satellite systems is analyzed in [31]. Jamming is characterized as the most critical threat for satellites in [48,66,76]. A new class of cyberattacks in space that leverages the communication between space assets, particularly satellites, to violate the availability and integrity of sensors and actuators used in space missions, is described in [80].

Loss of Control: The loss of control threat has been discussed by considering different attacker profiles in [53]. Loss of control can be caused by several cyber attacks on satellites. Such attacks are jamming, spoofing, or denial of service, that may disrupt communications, data processing, or the physical functions of the satellite. Furthermore, the loss of control threat in internet-connected satellites is analyzed considering four categories of threats in [83]. The criticality of loss of control in satellites is examined in [48,85].

Information Disclosure The information disclosure threat is among the most common threats in satellites according to [84]. The leak of information in satellites can be performed by leveraging vulnerabilities in a satellite receiver dish and software to perform a spectrum analysis. To this end, an adversary could determine if a transponder is operational or if it has unused bandwidth and power and attack on the excess capacity. Thereafter, this attack may cause denial of service or the unintentional transmission of illegal signals. General aspects of the information disclosure threat in satellites are discussed in [71,73]. Further, the information disclosure threat against satellites is analyzed in [75] considering the space, ground, link, and user segments. The information disclosure threat that targets the signals in satellites is discussed in [82]. The realization of the threat by using malware is analyzed in [48,50,68,74–76]. Additionally, eavesdropping attacks that may result in information disclosure are studied in [31,60,70,79,82,84,86,87]. The information disclosure threat in small satellites is analyzed in [74], where hardware, software, and network vulnerabilities have been considered. Information disclosure attack scenarios are discussed in [71], where space assets, attack motivation, and attacker profiles are analyzed. The criticality of the information disclosure threat in satellites is discussed and assessed in [48,60,73,76,79]. Eavesdropping attacks are characterized as the most critical for satellites in [31]. By leveraging the STRIDE methodology, the eavesdropping attack is analyzed in [86]. The leak of information in satellite communications is analyzed in [87] towards identifying the most efficient mitigation technique.

Denial of Service: The denial of service threat has been classified among the most common threats in satellites [84]. General discussions about the threat in satellites are provided in [31,49,62,63,66,70–73,75,76,79,82,84,86,88,89]. The denial of service attack could block the operations of network-based services, affecting the control operations or data transfer to and from a satellite, leading to the loss of the asset. The denial of service threat in satellites is analyzed in [75,86] considering the space, ground, link, and user segments. Therein, the space assets, attack motivations, and attacker profiles for a denial of service attack are analyzed by leveraging the STRIDE method. Moreover, the threats in satellites considering the space, link, and ground segments are presented in [89]. Following a systematic analysis, the STRIDE and DREAD methods are utilized to analyze denial of service threats in satellites [73]. The denial of service threat against small satellites is briefly discussed in [74] considering hardware, software, and network vulnerabilities. A brief description of the threat in small satellites is provided in [70]. Denial of service caused by malware is studied in [48,50,68,74–76]. Additionally, the denial of service attacks in satellites are partially discussed in [48,50]. The impact of a denial of service attack in the four space segments of a satellite is analyzed in [66] by means of examining ten denial of service attack scenarios. The Denial of service threat is among the most critical ones for satellites; its criticality is discussed in [31,72,76,79,85,88]. The denial of service attack is characterized as the most critical threat for satellites, as availability is a top priority in the domain [49]. Such attacks in satellites and in cubesats are analyzed in [62,63] and the same attack on the satellite payload is analyzed in [82]. The ViaSat cyberattack is analyzed in [68], where the malware wiper that targeted the ground segment to disrupt the communications of the satellite infrastructure is presented. The attack leveraged network and VPN vulnerabilities to upload the malware. The technical and organizational aspects and lessons learnt are described in relation to the cyber attack's lifecycle.

Elevation of Privilege: The elevation of privilege attacks against satellites are analyzed in [31,61,71–73,76,82,86]. The elevation of privilege can be performed through entry points such as I/O ports and wireless communications and affects the satellite's onboard sensors. The attacker gains unauthorized access to the satellite systems and performs malicious actions, such as turning off critical components [71,86]. This threat in satellites has been systematically analyzed by leveraging the STRIDE method and the attack motives and the attacker profiles have been considered in [71,86]. Both the STRIDE and DREAD methods have been applied to satellite assets to discuss security threats including elevation of privileges in [73]. By leveraging the NIST cybersecurity framework, the elevation of privileges attack in satellites is discussed in [76]. A satellite payload attack is described in [82]. The impact of the elevation of privileges attack in satellites is analyzed in [72], by utilizing the attack trees method. The criticality of the threat is discussed in [31,61].

Replay: Several works have discussed the replay attack against satellites: [31,49,65,75,76,82,90]. An attacker may compromise the system's functionality by modifying routing information and replaying old packets over the satellite network, thus causing malfunction in the communications between the satellite and the ground segment [90]. A general discussion about replay attacks in satellites is provided in [90] towards proposing an appropriate security mechanism to counter them. Further, replay attacks in satellites have been discussed in [75] considering the space, ground, link, and user segments. The criticality of the replay attack is discussed in [49,76] and [31] provides an overview of cybersecurity incidents in satellites where the replay attack is classified among the most critical threats. Replay attacks in satellite signals have been examined in [82]. The potential implications of the replay attack in the communications between satellites and ground stations are studied in [65].

4.2.2. Vulnerabilities

By leveraging the NASA open source core flight system, the network vulnerabilities are identified and four exploits are utilized in [65]. The focus was on the software bus (SB) and the communication between satellites and ground station and more specifically on the lack of authentication in SB and the lack of incident recovery plans through the SB entry point. By analyzing the user segment, the default credentials, weak encryption, insecure protocols, and software backdoor are characterized as the most common satellite vulnerabilities in [60]. On the other hand, the increasing adoption of COTS and legacy systems increases the attack surface and are among the most critical vulnerabilities in the space, link, and ground segments of satellites, according to [81]. Further, [91] identifies the adoption of legacy systems, the lack of regulations and standards, supply chain vulnerabilities, and the easiness to access space technology as the most critical vulnerabilities of satellite assets.

4.2.3. Risks

Cybersecurity risks in satellites are discussed in several works in the literature. The discussion is mostly about methods for risk management rather than detailed analysis of the risks themselves.

Risk-related methods: A risk management method for satellite systems is proposed in [91]. The method consists of the main risk management phases, namely threat identification, vulnerability analysis, risk assessment, risk mitigation, contingency plan, and incident response. However, specific cyber risks in satellite assets are not considered. An approach is proposed in [92] to facilitate the cyber risk governance in satellite. The approach takes into account the vulnerabilities, threat actors, targets, impact, and countermeasures. Furthermore, the NIST cybersecurity framework is proposed as an appropriate approach to analyze the risks of the unmanned commercial space vehicles. A small satellite vehicle is analyzed to illustrate the workings of the framework. Several cybersecurity threats, such as jamming, communication interception, data tampering, and denial of service, along with their impact and severity are analyzed. The interception/loss of sensor data, hijacking/unauthorized commands, and malicious code injections are characterized as the most critical risks. Finally, a set of recommendations is provided to mitigate the aforementioned risks. The risks of the space infrastructure and of satellites are analyzed in [76], by leveraging the NIST CSF. High risk levels exist for denial of service, sensor injection, and jamming. Eavesdropping, replay attack, and data manipulation are characterized as medium level risks. Although several of the reviewed works have followed a systematic method and have identified different levels of criticality, a comprehensive analysis of the risks that would provide details about the different risk management phases has not been made available.

Risk taxonomies: A security risk taxonomy for commercial space missions is provided in [62]. The risks have been categorized considering past incidents and existing databases and technical reports. Physical, digital, organizational, and regulatory risks are included; however, software related risks and mechanical faults are not included in the proposed taxonomy. Technical and social engineering categories that include signal hijacking, data manipulation, space situational awareness deception, seizure of control, denial of service, phishing and baiting are identified as cyber risks.

4.2.4. Countermeasures

Similarly to the threats and attacks, several works have analyzed countermeasures and security strategies for satellites. Fig. 9 presents the proposed countermeasures for satellites, following the NIST CSF core functions classification [54]. The majority of the countermeasures are related to the *protect*, *detect*, and *respond* functions, with only two out of sixty six reviewed articles discussing controls for recovery plans. However, the countermeasures for satellites capture more aspects than those for the space infrastructure (shown in Fig. 6).

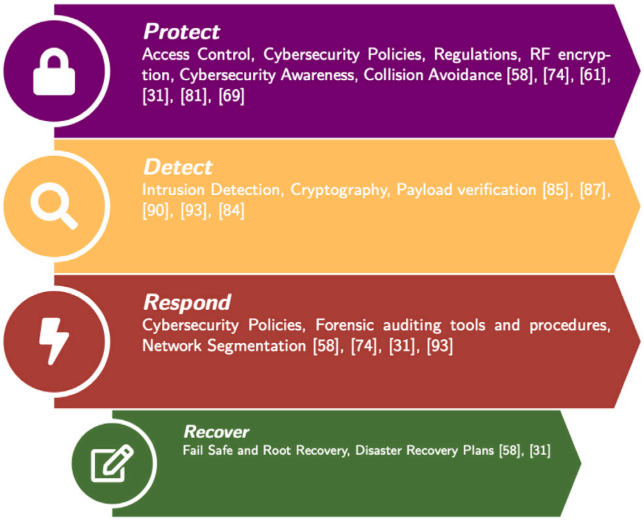

Protect
Access Control, Cybersecurity Policies, Regulations, RF encryption, Cybersecurity Awareness, Collision Avoidance [58], [74], [61], [31], [81], [69]
Detect
Intrusion Detection, Cryptography, Payload verification [85], [87], [90], [93], [84]
Respond
Cybersecurity Policies, Forensic auditing tools and procedures, Network Segmentation [58], [74], [31], [93]
Recover
Fail Safe and Root Recovery, Disaster Recovery Plans [58], [31]

Fig. 9. Countermeasures for satellites.

Protect: Several cybersecurity controls have been proposed to protect against cyberattacks in satellites [31,58,61,69,74,81]. A set of basic cybersecurity guidelines for small satellites that includes enforcement of cryptography, application of access control, and satellite operational procedures such as fail-safe and root recovery was proposed in [58]. Different encryption mechanisms to ensure the communication of the telemetry and telecommand in small satellites were analyzed in [74]. The analysis concluded that AES-128 is among the most secure and energy-efficient algorithms for small satellites. Recommendations that focus on satellite space and ground systems are discussed in [31]; these are: RF encryption; specialized ground station hardware; use of forensic auditing tools and procedures; enable the monitoring of behavioral anomalies by leveraging intrusion detection systems; store a verified secure copy of the satellite operating system on a trusted platform module (TPM); continuously patch hardware and software vulnerabilities; formal verification of the code in the payload; increase redundancy in the case of compromise or loss; encryption of communications; and develop disaster recovery plans. Further, security awareness and cybersecurity standards and regulations are among the basic means of protecting satellite assets [81]. A cybersecurity scheme to mitigate the eavesdropping threat is proposed in [87], where the Low-Density Parity-Check (LDPC) coding is employed to ensure the confidentiality of communication by leveraging channel uniqueness information into the coding process. Following a similar approach, a security mechanism for satellite networks, based on blockchain, is proposed in [90], where techniques such as access control, confidentiality, and security authentication are proposed to mitigate unauthorized access, non-repudiation, false data injection, and replay attacks. Finally, a collision avoidance system for satellites was proposed in [69]. This system aims to protect satellites against indirect kinetic cyber attacks that can result in a collision; such an attack is spoofing. Several general recommendations were proposed in [61] to protect satellites. Among these, access control mechanisms, strong cybersecurity regulations, and cybersecurity policies are the baseline measures.

Detect: To facilitate the detection of cyberattacks in satellites, security mechanisms such as intrusion detection and payload verification have been proposed [84,85,87,90,93]. A novel intrusion detection system for satellite systems that operates over the routing protocols is proposed in [85]; this control aims to mitigate DoS attacks in dynamic space information networks. By analyzing the resilience of satellite assets, advanced algorithms were developed to create adversarial networks (for attack simulation purposes), variational auto-encoders, and multi-variate time-series in [93]. This facilitates the development of cyber resilient technologies and particularly intrusion detection systems and automated threat response to mitigate injection attacks. Furthermore, an intrusion detection scheme for IoT-based satellite networks is proposed in [84] to mitigate denial of service, power depletion, and eavesdropping attacks. Finally, the resilience of satellite assets is examined in [93] by proposing cybersecurity countermeasures such as variational auto-encoders, and multi-variate timeseries.

Respond: Practices such as cybersecurity policies, audits, and reactive network segmentation have been proposed to respond in case of a cyber incident [31,58,74,93]. A set of basic cybersecurity guidelines for small satellites including cybersecurity policies and auditing procedures focusing on cyber incident response are proposed in [58]. Increase redundancy in the case of compromise or loss and develop incident response plans are discussed in [31].

Recover: The recovery function of the NIST framework is only partially addressed in the proposed countermeasures [31,58], where a set of cybersecurity guidelines to ensure recovery in case of a cyber attack and policy development are proposed. The need to increase the redundancy in the case of compromise or loss and to develop disaster recovery plans is mentioned in [31].

4.2.5. Requirements

The cybersecurity requirements for satellites are partially analyzed without following a systematic method or approach for their elicitation. The importance of confidentiality, integrity, availability, authenticity, and safety to the satellite ecosystem is highlighted in [91]. It is important, according to the existing approaches, that the space assets fulfill the CIA triad requirements along with the authenticity of the transmitted data and the safety objective to avoid physical hazards. Further, a satellite supply chain cybersecurity framework based on the NIST SP 800-171 Rev.2 [94] requirements is proposed in [50], where the payload control center, hardware components, and embedded software are characterized as critical assets. By leveraging existing security requirements the security strengths and weaknesses of the satellite suppliers are examined and evaluated. The threats and attacks are identified by utilizing the STRIDE method, and authentication, integrity, non-repudiation, confidentiality, availability, and authorization are identified as the basic requirements for the satellite infrastructure [73].

4.2.6. Legal issues

Although space/satellite-specific acts and regulations exist, the cybersecurity of the space infrastructure and of satellites is only partially addressed, in the form of guidelines [95–98]. A typology of hostile events involving satellites, classified in three categories, namely kinetic, virtual, and hybrid events is provided in [99]. The UN Charter regime, Space law, and the telecommunication law are considered in this analysis to discuss the need for a global framework for multi-stakeholder cooperation. The governance and cooperation issues of cybersecurity of satellites are discussed along with the existing barriers towards developing cybersecurity governance procedures in [77]. The main security objectives regarding satellites of the European Space Agency (ESA) policy are discussed in [55]. Asset identification, requirements establishment, and the establishment of necessary procedures are among the most critical towards the development of standards and regulations. Additionally, the legal aspects that cyberattacks against satellites may pose are examined in [56]. Specifically, [56] discusses the existing legal frameworks and mechanisms for the cybersecurity of satellites, along with the national mechanisms of Australia and Ukraine. The important steps towards increasing the security posture in satellites include the establishment of requirements for technical standards, and the development of a legal culture for space cybersecurity. The EU new directives on Network and Information Security (NIS2) and on the Resilience of Critical Entities (RCE) and their relevance to the space infrastructure and in particular to satellite cybersecurity are examined in [64] to provide the current status of relevant legislation in the EU. An overview of the regulations and laws in cybersecurity regarding mega-constellations of satellites, potential risks per segment, and mitigation techniques is provided in [48], where the definitions of the main space-related terms in existing legal frameworks, along with the technical standards for the satellite assets is provided. Finally, the regulatory framework regarding space cybersecurity and particularly Article VI on satellite cybersecurity of the Outer Space Treaty (OST) are analyzed in [57].

5. Discussion and future research directions

A summary of the results presented in the previous section is shown in Tables 2 and 3. Table 2 provides a tabular overview of the results obtained from the systematic literature review. They are divided into four areas: year; country; cybersecurity aspects of focus; and type of the analyzed work.

Most (46) of the reviewed works discuss and analyze threats that might inflict damage to the space infrastructure. However, most of them contain general discussions, without systematically analyzing potential threats. Eighteen out of the reviewed sixty six papers elaborate on past or future cyberattacks; seven focus on space infrastructure assets and eleven on satellites. Only ten of the reviewed works provide information about the risk analysis and management processes. Most of those that do are based on the NIST CSF [54]. Thirty four out of the reviewed sixty six works discuss and propose cybersecurity controls or mitigation techniques for space infrastructure assets, while only nine papers analyze system vulnerabilities. Eleven works analyze cybersecurity legal aspects, focusing on the national and international regulations and the lack of both technical and regulatory standards. Last, only two works discuss cybersecurity requirements in the space domain. However, the discussion is on general concepts, such as the CIA triad, without employing a methodology to define requirements and ensure the application of cybersecurity by design principles.

Table 3 gives an overview of the cybersecurity threats that the reviewed works focus on. Three threats have been analyzed in most of the reviewed works, namely *jamming, spoofing,* and *denial of service*; twenty eight, twenty five, and twenty works have discussed such threats respectively. The denial of service threat in satellites is analyzed in seventeen out of twenty papers, possibly due to its criticality in communications and other critical infrastructure operations [18]. The *eavesdropping* and *privilege escalation* threats have been analyzed in eleven and ten works respectively. These threats are mostly analyzed in satellite systems and components, with only five works having discussed their impact on space infrastructure assets. The *malware* and *replay* attacks attracted the attention of nine and eight works respectively, with particular focus on satellites. Finally, the *tampering, loss of control*, and *information disclosure* threats for satellites are only scarcely analyzed in the literature. Five out of sixty six works have analyzed cyber threats by leveraging a systematic process or methodology [46,63,71,73,86]; STRIDE, DREAD, and the attack trees methods have been utilized. Further, four out of these five systematic analyses are focused on satellite components and only one approach is used to analyze threats in the space infrastructure. The denial of service, tampering and privilege escalation threats have been explored by three, one and two studies respectively, while in the satellite domain these threats have been extensively discussed.

Based on the results in Section 4 and the discussion above, the following future research directions are suggested:

Table 2
Summary overview of the SLR results.

	Year	Country	Cybersecurity Focus	Type
Space	2009 [32]	USA	Threats	Technical Report
	2014 [7]	USA	Attack, Threat	Article
	2016 [34]	UK	Countermeasures	Technical Report
	2016 [35]	EU	Threat	Technical Report
	2018 [2]	USA	Threats, Attacks, Countermeasures	Conference
	2018 [44]	EU	Threats, Countermeasures	Technical Report
	2019 [45]	UK	Threats, Countermeasures, Vulnerabilities	Technical Report
	2020 [53]	OC	Risk	Technical Report
	2020 [36]	EU	Countermeasures	Article
	2020 [46]	UK	Threats, Attacks	Conference
	2020 [37]	EU	Threats, Countermeasures, Requirements	Article
	2021 [38]	EU	Threats, Attacks, Countermeasures	Conference
	2021 [42]	UK	Threats, Attacks	Article
	2021 [39]	AS	Threats, Attacks	Conference
	2021 [51]	USA	Threats, Countermeasures	Technical Report
	2022 [40]	EU	Threats, Vulnerabilities, Legal issues	Technical Report
	2022 [41]	EU	Countermeasures, Vulnerabilities	Conference
	2022 [43]	EU	Threats, Vulnerabilities	Technical Report
	2022 [47]	EU	Threats, Countermeasures	Conference
Satellite	2014 [88]	USA	Threats	Conference
	2015 [85]	AS	Threats, Countermeasures	Article
	2016 [100]	USA	Countermeasures	Conference
	2016 [99]	AS	Legal issues	Article
	2017 [58]	USA	Countermeasures	Conference
	2018 [55]	EU	Legal issues	Article
	2018 [77]	EU	Legal issues	Technical Report
	2018 [78]	USA	Attacks	Technical Report
	2019 [59]	USA	Countermeasures, Threats, Risks	Technical Report
	2019 [91]	UK	Vulnerabilities, Requirements, Threats, Risks	Conference
	2019 [60]	UK	Attacks, Threats	Article
	2019 [74]	AS	Countermeasures	Article
	2019 [1]	UK	Threats, Attacks, Vulnerabilities	Conference
	2020 [61]	USA	Threats, Countermeasures	Article
	2020 [92]	USA	Risks	Article
	2020 [79]	AS	Threats	Article
	2020 [31]	UK	Threats, Countermeasures	Article
	2020 [86]	UK	Threats, Attacks	Conference
	2020 [80]	USA	Attacks	Conference
	2021 [62]	USA	Risks	Conference
	2021 [81]	USA	Countermeasures, Vulnerabilities, Threats	Technical Report
	2021 [87]	USA	Countermeasures	Article
	2021 [63]	USA	Attack, Threats, Countermeasures	Conference
	2021 [82]	UK	Threats	Technical Report
	2021 [90]	AS	Countermeasure	Conference
	2021 [70]	USA	Risks	Technical Report
	2021 [93]	USA	Countermeasures	Conference
	2021 [75]	OC	Countermeasures, Threats	Article
	2021 [56]	EU	Legal issues	Article
	2021 [83]	EU	Threats	Technical Report
	2021 [64]	EU	Legal issues	Technical Report
	2022 [65]	USA	Vulnerabilities	Conference
	2022 [84]	OC	Countermeasures	Article
	2022 [71]	USA	Threats, Countermeasures	Conference
	2022 [76]	EU	Risks	Technical Report
	2022 [66]	OC	Threats, Countermeasures	Conference
	2022 [67]	EU	Countermeasures, Threats	Article
	2022 [68]	USA	Attacks	Conference
	2022 [89]	USA	Threats, Education	Conference
	2022 [72]	USA	Attacks	Conference
	2022 [69]	CA	Countermeasure	Article
	2022 [73]	UK	Threats, Requirements	Article
	2022 [48]	A, EU	Legal issues	Article
	2022 [101]	USA	Attacks, Countermeasures	Conference
	2023 [57]	AS	Legal issues	Article
	2023 [49]	EU	Threats, Education	Conference
	2023 [50]	USA	Risks	Article

- **Security by design:** Vulnerabilities and threats in space assets may arise during all phases of a system's lifecycle. However, improving the cybersecurity posture of a system early in the development and production phases reduces the attack surface and consequently the cyber risks. The increasing adoption of COTS components, the commercialization of the sector, and the increasing dependence on software applications create the need to define and apply cybersecurity by design principles for the overall space infrastructure. More research is needed to provide actionable guidance on this.
- **Threats, vulnerabilities, attacks and requirements analysis in the space infrastructure:** The systematic analysis of threats in the space infrastructure provides a comprehensive understanding of the space threat landscape. This process facilitates the

Table 3
Overview of cyber threats in space.

	Reference	Spoofing	Malware	Eavesdropping	Denial of service	Jamming	Tampering	Replay	Loss of control	Information disclosure	Privilege escalation
Space	[32]	✓				✓					
	[7]	✓									✓
	[34]	✓				✓					
	[35]	✓			✓						
	[2]	✓									
	[44]					✓					
	[45]				✓	✓		✓			
	[53]										
	[36]	✓									
	[46]										✓
	[37]	✓			✓	✓			✓		
	[38]	✓									
	[42]			✓		✓	✓				
	[39]	✓				✓					
	[51]										
	[40]	✓	✓	✓		✓					
	[41]	✓									
	[43]					✓					
	[47]		✓	✓		✓					
	[88]		✓								
Satellite	[85]				✓						
	[100]								✓		
	[99]										
	[58]					✓					
	[55]	✓									
	[77]					✓					
	[78]					✓					
	[59]								✓		
	[91]	✓									
	[60]			✓		✓					
	[74]	✓	✓			✓					
	[1]										
	[61]										✓
	[92]	✓									
	[79]			✓	✓	✓					
	[31]			✓	✓	✓		✓			✓
	[86]	✓		✓	✓						✓
	[80]					✓					
	[62]				✓						
	[81]	✓				✓					
	[87]			✓							
	[63]				✓		✓				
	[82]	✓		✓	✓	✓		✓			✓
	[90]							✓			
	[70]			✓	✓	✓	✓				
	[93]										
	[75]		✓		✓			✓			
	[56]										
	[83]	✓				✓			✓		
	[64]					✓					
	[65]	✓						✓			
	[84]	✓		✓	✓	✓					
	[71]				✓	✓	✓			✓	✓
	[76]		✓		✓	✓		✓			✓
	[66]				✓	✓					
	[67]	✓									
	[68]	✓	✓								
	[89]	✓			✓						
	[72]				✓		✓				✓
	[69]										
	[73]	✓			✓		✓			✓	✓
	[48]		✓			✓			✓		
	[101]										
	[57]										
	[49]				✓			✓			
	[50]		✓								
Sum		25	9	11	20	28	6	8	5	2	10

identification of critical space components, the cyber risks, and potential countermeasures. The payload in space assets provides critical mission data by communicating to the ground station. Analyzing the cybersecurity threats and vulnerabilities of the payload facilitates the identification of the most appropriate security techniques for space assets and informs the elicitation of requirements, which in turn is the basis for defining a cybersecurity reference architecture for the four segments of the space infrastructure. More research is needed on the assessment and treatment of cybersecurity risk in space infrastructure, by studying and adopting existing frameworks for both information technology [102–105] and cyber–physical systems [106].

- **Interconnections and interdependencies in Space:** Interconnections and interdependencies within and between space segments and other critical infrastructures need to be identified and analyzed. This will allow the identification of the information and control flows between cyber–physical systems that comprise the space, link, ground, and user segments. Such analysis allows the complete specification of the space infrastructure reference architecture that in turns informs the accurate assessment of risks. To this end, more research is needed in the identification of interconnections and interdependencies between space systems to systematically analyze the overall space ecosystem and identify vulnerability inheritance, threat and risk propagation, and the most appropriate security controls for space. By leveraging existing systematic methodologies [107,108], the interconnections and interdependencies in space can be explored.
- **Cybersecurity framework:** The unique characteristics of space create the need to develop a comprehensive cybersecurity framework to manage the attendant cyber risks. Such a framework will provide risk management procedures to deal with unique space characteristics such as the single point of failure, lack

of standards and regulations, complex supply chain, and the widespread adoption of COTS. Further, through this framework, a set of cybersecurity best practices for all four space segments will be provided, towards improving the cybersecurity posture in the space infrastructure.

- **Human interactions:** The number of spaceflight missions involving and/or carrying humans grows rapidly. Therefore, it is of paramount importance to analyze human aspects and interaction with and among humans in the space infrastructure, considering the four space segments and safety issues too. The resolution of conflicting safety and cybersecurity requirements needs to be examined, to identify avenues towards developing safe and cyber secure missions. Additionally, the threats and risks that might arise because of the human interactions should be analyzed.
- **Cybersecurity standards and regulations:** Even though space is a highly standardized domain, there is a lack of cybersecurity-specific standards and regulations. The adoption of industry standards and guidelines to improve the cybersecurity posture in space is needed; this process can be greatly facilitated and informed by research.
- **Cascade effects:** The short and long term cascading effects of cyberattacks in space on other critical infrastructures need to be considered, by means of a systemic risk assessment approach. More research is needed in analyzing the interconnections between critical infrastructures and space infrastructure. Further, the risk propagation between these would increase the cybersecurity posture of the space infrastructure and hence of the interconnected critical infrastructures.

6. Conclusions

In this paper we answered the posed research questions by conducting a systematic literature review that summarized and organized recent research results on the cybersecurity in the space infrastructure at large and in satellites in particular, to integrate and add understanding to existing work in the field. Research on the topic is increasing, as more interconnected, advanced systems are included in the space infrastructure. Following a systematic approach we identified and analyzed sixty six relevant publications. The majority of the reviewed studies focus on satellites and their communication components and only partially study the cybersecurity of cyber–physical systems in both the space and ground segments. Although several works have examined threats, vulnerabilities, attacks, and risks, a comprehensive analysis that will include and combine these aspects and will consider the unique operations and conditions in space, is still needed. Such analysis should extend to all four space segments and lead to the formulation of a cybersecurity framework based on the NIST CSF. Given the international nature of space, such an endeavor will best be undertaken by leveraging international collaborations and by sharing cybersecurity knowledge.

Funding

This work was supported (a) by the Research Council of Norway [grant number 310105 “Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS”] and (b) by the European Commission [grant 101120657 “European Lighthouse to Manifest Trustworthy and Green AI” - ENFIELD].

CRediT authorship contribution statement

Georgios Kavallieratos: Conceptualization, Methodology, Validation, Investigation, Data curation, Writing – original draft, Visualization. **Sokratis Katsikas:** Conceptualization, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Sokratis Katsikas reports financial support was provided by Research Council of Norway. Georgios Kavallieratos reports financial support was provided by the European Commission [“European Lighthouse to Manifest Trustworthy and Green AI” - ENFIELD].

Data availability

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

References

[1] J. Pavur, I. Martinovic, The cyber-ASAT: On the impact of cyber weapons in outer space, in: 2019 11th International Conference on Cyber Conflict, Vol. 900, CyCon, IEEE, 2019, pp. 1–18.

[2] G. Falco, The vacuum of space cyber security, in: 2018 AIAA SPACE and Astronautics Forum and Exposition, 2018, p. 5275.

[3] A. Georgescu, U.-E. Botezatu, A.-D. Popa, Ş. Popa, Ş.-C. Arseni, Critical infrastructure dependency on space systems, Mircea cel Batran XIX (2015) 399–404.

[4] Orbiting now, 2023, URL: https://orbit.ing-now.com/.

[5] C.S. Cerqueira, W.A. dos Santos, A.M. Ambrosio, Development of an interface to a spacecraft simulator empowered by virtual reality, SBC J. Interact. Syst. 3 (3) (2012) 37–44.

[6] New Space Economy, Space system segments – A quick overview, 2023, [online] https://newspaceeconomy.ca/2023/02/02/space-system-segments-a-quick-overview/. (02 February 2023).

[7] D. Byrne, D. Morgan, K. Tan, B. Johnson, C. Dorros, Cyber defense of space-based assets: verifying and validating defensive designs and implementations, Procedia Comput. Sci. 28 (2014) 522–530.

[8] R. Santamarta, A wake-up call for satcom security, in: Technical White Paper, IOActive, 2014, [online] https://www.secnews.gr/wp-content/uploads/Files/Satcom_Security.pdf. (05 July 2023).

[9] L.-K. Hlavica, Hacker-Attacks Against Satellites (Master’s thesis), International Technology Law, Vrije Universiteit Amsterdam, 2021.

[10] D. Goward, Mass GPS spoofing attack in black sea? 2017, [online] https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea. (03 May 2023).

[11] P.K. Martin, Inspector General, NASA cybersecurity: An examination of the agency’s information security, in: NASA, Testimony Before the Subcommittee on Investigations and Oversight, US House of Representatives, House Committee on Science, Space, and Technology, Vol. 29, 2012.

[12] A. Corallo, A.M. Crespino, V. Del Vecchio, M. Lazoi, M. Marra, Understanding and defining dark data for the manufacturing industry, IEEE Trans. Eng. Manage. 70 (2021) 700–712.

[13] B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical-layer security in space information networks: A survey, IEEE Internet Things J. 7 (1) (2019) 33–52.

[14] M. Zhuo, L. Liu, S. Zhou, Z. Tian, Survey on security issues of routing and anomaly detection for space information networks, Sci. Rep. 11 (22261) (2021) http://dx.doi.org/10.1038/s41598-021-01638-z.

[15] M. Höyhtyä, S. Boumard, A. Yastrebova, P. Järvensivu, M. Kiviranta, A. Anttonen, Sustainable satellite communications in the 6G era: A European view for multi-layer systems and space safety, IEEE Access 10 (2022) 99973–100005, http://dx.doi.org/10.1109/ACCESS.2022.3206862.

[16] J. Pavur, I. Martinovic, Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, J. Cybersecur. 8 (1) (2022) http://dx.doi.org/10.1093/cybsec/tyac008.

[17] W. Jiang, Software defined satellite networks: A survey, Digit. Commun. Netw. (2023) http://dx.doi.org/10.1016/j.dcan.2023.01.016

[18] N. Abdelsalam, S. Al-Kuwari, A. Erbad, Physical layer security in satellite communication: State-of-the-art and open problems, 2023, arXiv preprint arXiv:2301.03672, URL: https://api.semanticscholar.org/CorpusID:255570125.

[19] Y. Yan, G. Han, H. Xu, A survey on secure routing protocols for satellite network, J. Netw. Comput. Appl. 145 (2019) 102415, http://dx.doi.org/10.1016/j.jnca.2019.102415.

[20] P. Tedeschi, S. Sciancalepore, R. Di Pietro, Satellite-based communications security: A survey of threats, solutions, and research challenges, Comput. Netw. (2022) 109246.

[21] E. Bell, A. Bryman, B. Harley, Business Research Methods, Oxford University Press, 2022.

[22] J.W. Creswell, C.N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, Sage publications, 2016.

[23] T.C. Lacerda, C.G. von Wangenheim, Systematic literature review of usability capability/maturity models, Comput. Stand. Interfaces 55 (2018) 95–105, http://dx.doi.org/10.1016/j.csi.2017.06.001.

[24] A. Fink, Conducting Research Literature Reviews: From the Internet to Paper, Sage publications, 2019.

[25] C. Okoli, K. Schabram, A guide to conducting a systematic literature review of information systems research, SSRN Electron. J. 10 (2010) http://dx.doi.org/10.2139/ssrn.1954824.

[26] H.J. Ofte, S. Katsikas, Understanding situation awareness in SOCs, A systematic literature review, Comput. Secur. (2022) 103069, http://dx.doi.org/10.1016/j.cose.2022.103069.

[27] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, Int. J. Surg. 88 (2021) 105906.

[28] K. Kannelønning, S.K. Katsikas, A systematic literature review of how cybersecurity-related behavior has been assessed, Inf. Comput. Secur. (2023).

[29] V. Kampourakis, V. Gkioulos, S. Katsikas, A systematic literature review on wireless security testbeds in the cyber-physical realm, Comput. Secur. (2023) 103383.

[30] R. Silva, F. Neiva, Systematic Literature Review in Computer Science—A Practical Guide, Federal University of Juiz de Fora Technical Report of Computer Science Department, 2016, http://dx.doi.org/10.13140/RG.2.2.35453.87524.

[31] J. Pavur, I. Martinovic, Sok: Building a launchpad for impactful satellite cyber-security research, 2020, http://dx.doi.org/10.48550/arXiv.2010.10872, arXiv preprint arXiv:2010.10872.

[32] B. Garino, J. Gibson, Space system threats, AU-18 Space Primer (2009) 273–281.

[33] P.A. Slann, Anticipating uncertainty: The security of European critical outer space infrastructures, Space Policy 35 (2016) 6–14.

[34] D. Livingstone, P. Lewis, Space, The Final Frontier for Cybersecurity? Chatham House. The Royal Institute of International Affairs, 2016.

[35] M. Pellegrino, G. Stang, Space security for Europe, EU Inst. Secur. Stud. 19 (2016) 99.

[36] M. Polkowska, Space situational awareness (SSA) for providing safety and security in outer space: implementation challenges for Europe, Space Policy 51 (101347) (2020) http://dx.doi.org/10.1016/j.spacepol.2019.101347.

[37] S. Zatti, Space and cyber threats, in: Handbook of Space Security: Policies, Applications and Programs, Springer, 2020, pp. 245–263.

[38] J. Pražák, Space cyber threats and need for enhanced resilience of space assets, in: European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2021, pp. 542–548, http://dx.doi.org/10.34190/EWS.21.006.

[39] G.P. Kumar, Space and cyber warfare: An umbilical bond, Cent. Land Warf Stud. (2021) 15.

[40] L. Palmqvist, H. Nilsson, A Multidisciplinary Analysis of Cyber Security in the Swedish Space Industry: Evaluating the Possibilities for Stakeholder Cooperation and Distributed Ledger Technology (Master's thesis), Upsala universitet, 2022.

[41] P. Breda, R. Markova, A. Abdin, D. Jha, A. Carlo, N.P. Mantı, Cyber vulnerabilities and risks of AI technologies in space applications, in: 73rd International Astronautical Congress, IAC, Paris, France, 2022.

[42] M. Manulis, C.P. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber security in new space: analysis of threats, key enabling technologies and challenges, Int. J. Inf. Secur. 20 (2021) 287–311.

[43] Northern Sky Research, Space Cybersecurity Current State and Future Needs, Technical Report, Northern Sky Research - White Paper, 2022, p. 13, [online] https://www.nsr.com/wp-content/uploads/2022/04/NSR-Space-Cybersecurity-White-Paper-FINAL.pdf. (02 June 2023).

[44] G. Pavesi, S. Plattard, S. Moranta, L. Perrichon, M. Sarret, Security in Outer Space: Rising Stakes for Europe, Vol. 64, European Space Policy Institute, 2018, p. 81.

[45] B. Unal, Cybersecurity of NATO's Space-Based Strategic Assets, Chatham House. The Royal Institute of International Affairs, 2019.

[46] C. Maple, M. Bradbury, H. Yuan, M. Farrell, C. Dixon, M. Fisher, U.I. Atmaca, Security-minded verification of space systems, in: 2020 IEEE Aerospace Conference, IEEE, 2020, pp. 1–13.

[47] V. Varadharajan, N. Suri, Security challenges when space merges with cyberspace, 2022, arXiv preprint arXiv:2207.10798.

[48] D. Jha, N.P. Manti, A. Carlo, L.C. Zarkan, P. Breda, A. Jha, Safeguarding the final frontier: Analyzing the legal and technical challenges to mega-constellations, J. Space Saf. Eng. 9 (4) (2022) 636–643.

[49] A. Costin, H. Turtiainen, S. Khandker, T. Hämäläinen, Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications, 2023, arXiv preprint arXiv:2302.08359.

[50] C. Fleming, M. Reith, W. Henry, Securing commercial satellites for military operations: A cybersecurity supply chain framework, in: International Conference on Cyber Warfare and Security, Vol. 18, No. 1, 2023, pp. 85–92.

[51] National Aeronautics and Space Administration, NASA's Cybersecurity Readiness, NASA Office of Inspector General Office of Audits Report No. IG-21-019, 2021, p. 32.

[52] J.G. Oakley, Cybersecurity for Space: Protecting the Final Frontier, A Press, 2020.

[53] M.D. Bilodeau, The Risk That Cyber-Attacks Pose to Outer Space Assets: How Can International Dialogue and Cooperation Help? (Master's thesis), McGill University, Canada, 2020.

[54] Critical Infrastructure Cybersecurity, Framework for Improving Critical Infrastructure Cybersecurity, Technical Report 4162018, 2018, [online] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.

[55] C. Giannopapa, M. Adriaensen, N. Antoni, K.-U. Schrogl, Elements of ESA's policy on space and security, Acta Astronaut. 147 (2018) 346–349.

[56] A. Hurova, Liability for cyber attacks on space objects, Czech Yearb. Int. Law XII (2021) 36.

[57] D. Li, Cyber-attacks on space activities: Revisiting the responsibility regime of article VI of the outer space treaty, Space Policy 63 (2023) 101522.

[58] K.W. Ingols, Design for security: Guidelines for efficient, secure small satellite computation, in: 2017 IEEE MTT-S International Microwave Symposium, IMS, IEEE, 2017, pp. 226–228.

[59] K. Ingols, R. Skowyra, Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program, Technical Report, MIT Lincoln Laboratory Lexington United States, 2019.

[60] D. Bird, Cybersecurity considerations for internet of things small satellite systems, Curr. Anal. Commun. Eng. J. 2 (2019) 69–79.

[61] H. Caudill, Big risks in small satellites: The need for secure infrastructure as a service, in: ASCEND 2020, 2020, p. 4017.

[62] G. Falco, N. Boschetti, A security risk taxonomy for commercial space missions, in: ASCEND 2021, 2021, p. 4241.

[63] 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, pp. 68–76.

[64] K. Bussov, Cybersecuring European Union Space Assets (Master's thesis), Tallonn University of Technology, 2021.

[65] A. Schalk, L. Brodnik, D. Brown, Analysis of vulnerabilities in satellite software bus network architecture, in: MILCOM 2022-2022 IEEE Military Communications Conference, MILCOM, IEEE, 2022, pp. 350–355.

[66] K. Thangavel, J.J. Plotnek, A. Gardi, R. Sabatini, 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, pp. 1–10.

[67] C. Van Camp, W. Peeters, A world without satellite data as a result of a global cyber-attack, Space Policy 59 (2022) 101458.

[68] N. Boschetti, N.G. Gordon, G. Falco, Space cybersecurity lessons learned from the ViaSat cyberattack, in: ASCEND 2022, 2022, p. 4380.

[69] M. Amin Alandihallaj, N. Assadian, K. Khorasani, Stochastic model predictive control-based countermeasure methodology for satellites against indirect kinetic cyber-attacks, Internat. J. Control (2022) 1–14.

[70] M. Scholl, Introduction to Cybersecurity for Commercial Satellite Operations, Technical Report, National Institute of Standards and Technology, 2022.

[71] R. Hasan, R. Hasan, Towards a threat model and security analysis of spacecraft computing systems, in: 2022 IEEE International Conference on Wireless for Space and Extreme Environments, WiSEE, IEEE, 2022, pp. 87–92.

[72] A.D. Santangelo, G. Falco, A. Viswanathan, The LinkStar cybersecurity "Sandbox", a platform to test small satellite vulnerabilities within the community–updates and lessons learned, in: AIAA SCITECH 2022 Forum, 2022, p. 0239.

[73] U.I. Atmaca, C. Maple, G. Epiphaniou, et al., Challenges in threat modelling of new space systems: A teleoperation use-case, Adv. Space Res. 70 (8) (2022) 2208–2226.

[74] S.S. Saha, S. Rahman, M.U. Ahmed, S.K. Aditya, Ensuring cybersecure telemetry and telecommand in small satellites: recent trends and empirical propositions, IEEE Aerosp. Electron. Syst. Mag. 34 (8) (2019) 34–49.

[75] E. Verco, Satellites are cyber insecure: We need regulation to avoid a disaster, ANU J. Law Technol. 2 (2) (2021).

[76] B.D. Zachar, Analysis and Risk Assessment of Malicious Cyber Activity Against Space Systems (Master's thesis), Masaryk University, Department of Political Science, 2023.

[77] L. Perrichon, Cybersecurity for Outer Space-A Transatlantic Study (Master's thesis), Univerzita Karlova, Fakulta sociálních věd, 2018.

[78] G. Falco, Job One for Space Force: Space Asset Cybersecurity, Vol. 79, Belfer Center, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2018.

[79] S. Bonnart, A. Pickard, N.P. Mantı, D. Jha, The mission as a tree: A novel approach to identifying cyber threats to satellites, IAC-20 E 9 (2020) 2.

[80] G. Falco, When satellites attack: Satellite-to-satellite cyber attack, defense and resilience, in: ASCEND 2020, 2020, p. 4014.

[81] B. Vollmer, NATOs mission-critical space capabilities under threat: Cybersecurity gaps in the military space asset supply chain, 2021, arXiv preprint arXiv:2102.09674.

[82] J. Pavur, Securing New Space: On Satellite Cyber-Security (Ph.D. thesis), University of Oxford, 2021.

[83] V.-C. Matei, Cybersecurity Analysis for the Internet-Connected Satellites (Master's thesis), Upsala Universitet, 2021.

[84] N. Moustafa, I.A. Khan, M. Hassanin, D. Ormrod, D. Pi, I. Razzak, J. Slay, DFSat: Deep federated learning for identifying cyber threats in IoT-based satellite networks, IEEE Trans. Ind. Inform. (2022).

[85] C. Jiang, X. Wang, J. Wang, H.-H. Chen, Y. Ren, Security in space information networks, IEEE Commun. Mag. 53 (8) (2015) 82–88.

[86] M. Bradbury, C. Maple, H. Yuan, U.I. Atmaca, S. Cannizzaro, Identifying attack surfaces in the evolving space industry using reference architectures, in: 2020 IEEE Aerospace Conference, IEEE, 2020, pp. 1–20.

[87] R. Geng, N. Ye, J. Liu, D. Zhu, Towards channel state information based coding to enhance security in satellite communication, J. Syst. Archit. 112 (2021) 101843.

[88] R.M. McGraw, M.J. Fowler, D. Umphress, R.A. MacDonald, Cyber threat impact assessment and analysis for space vehicle architectures, in: Sensors and Systems for Space Applications VII, Vol. 9085, SPIE, 2014, pp. 131–141.

[89] G. Hills, J. Baldasare, W. Henry, W. Connell, A customized approach to cybersecurity education for space professionals, in: MILCOM 2022-2022 IEEE Military Communications Conference, MILCOM, IEEE, 2022, pp. 160–165.

[90] C. Li, L. Zhu, M. Luglio, Z. Luo, Z. Zhang, Research on satellite network security mechanism based on blockchain technology, in: 2021 International Symposium on Networks, Computers and Communications, ISNCC, IEEE, 2021, pp. 1–6.

[91] C. Kapalidis, C. Maple, M. Bradbury, M. Farrell, M. Fisher, Cyber Risk Management in Satellite Systems, IET, 2019, pp. 1–8, http://dx.doi.org/10.1049/cp.2019.0139.

[92] B. Karabacak, G. Ikitemur, A. Igonor, A mixed public-private partnership approach for cyber resilience of space technologies, Frankl. Univ. Sch. Exch. (2020).

[93] M.G. Sahakian, S. Musuvathy, J. Thorpe, S. Verzi, E. Vugrin, M. Dykstra, Threat data generation for space systems, in: 2021 IEEE Space Computing Conference, SCC, IEEE, 2021, pp. 100–109.

[94] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, G. Guissanie, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Technical Report SP800-171 Rev.2, 2020, [online] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[95] Green Book, Security Threats Against Space Missions, Technical Report, CCSDS Secretariat, Washington, DC, USA, 2022.

[96] Green Book, Security Guide for Mission Planners, Technical Report, CCSDS Secretariat, Washington, DC, USA, 2019.

[97] Magenta Book, Security Architecture for Space Data Systems, Technical Report, CCSDS Secretariat, Washington, DC, USA, 2012.

[98] Green Book, The Application of Security to CCCDS Protocols, Technical Report, CCSDS Secretariat, Washington, DC, USA, 2019.

[99] D. Housen-Couriel, Cybersecurity threats to satellite communications: Towards a typology of state actor responses, Acta Astronaut. 128 (2016) 409–415.

[100] D.E. Cunningham, G. Palavincini Jr., J. Romero-Mariona, Towards effective cybersecurity for modular, open architecture satellite systems, 2016.

[101] S. Pazouki, A. Aydeger, Securing international space station against recent cyber threats, in: Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 3, Springer, 2022, pp. 121–132.

[102] International Organization for Standardization, ISO, ISO/IEC 27001:2013 information technology — Security techniques — information security management systems — Requirements, 2013.

[103] International Organization for Standardization, ISO, ISO/IEC 27002:2013 information technology security techniques code of practice for information security controls, 2013.

[104] International Organization for Standardization, ISO, ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018.

[105] International Organization for Standardization, ISO, ISO 31000:2018 Risk management — Guidelines, 2018.

[106] E.R. Griffor, C. Greer, D.A. Wollman, M.J. Burns, Framework for cyber-physical systems: Volume 2, working group reports, 2017.

[107] G. Kavallieratos, G. Spathoulas, S. Katsikas, Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems, Sensors 21 (5) (2021) 1691.

[108] A. Akbarzadeh, Dependency Based Risk Analysis in Cyber-Physical Systems, NTNU, 2023.