Computers & Security 140 (2024) 103799

Contents lists available at ScienceDirect

Computers & Security

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

Securing SatCom user segment: A study on cybersecurity challenges in view of *IRIS*^{2}

Francesco Casaril [a], Letterio Galletta [a,b,*]

[a] *IMT School for Advanced Studies Lucca, Lucca, Italy*
[b] *CINI Cybersecurity National Laboratory, Rome, Italy*

ARTICLE INFO

Keywords:
Satellite cybersecurity
SatCom
Space infrastructure
Risk management
Modem security

ABSTRACT

The advancement in communications technologies and recent geopolitical events highlighted the need for fast and reliable satellite communications infrastructure for military and civil security operations. Starting from the case study of the Viasat cyberattack in February 2022, this paper analyzes the common vulnerabilities of the ground and, in particular, user segments in SatCom infrastructures, focusing on modems security, and proposes some best practices and solutions in the field of risk management to prevent such attacks. Moreover, the research compares the standards and the guidelines used in the United States concerning routers and network security with those in the European Union. Our findings highlight the need for clear and effective standards or certification schemes to cyber-proof the new components of *IRIS*^{2}, the "Infrastructure for Resilience Interconnectivity and Security by Satellite", Europe's first multi-orbital satellite constellation. This need becomes more compelling, especially in view of the entry into force of the Network and Information Security Directive or NIS2 Directive. We conclude by discussing future research directions and emerging trends in cyber risk management for the SatCom user segment. This paper aims to provide valuable insights into managing cyber risks in critical space infrastructure and can inform future efforts to improve cybersecurity in view of *IRIS*^{2}.

1. Introduction

Space has become indispensable for economic and social development on Earth, but at the same time, it is a new field of confrontation. Historically contained in the three domains, air-land-sea, strategic confrontation is expanding to new fields: cyberspace, space, and cognitive. Competition, combined with the emergence of new disruptive technologies, means that the prospect of true space warfare is becoming less and less hypothetical (Rementeria, 2022). Despite the principle of peaceful use of space, as declared by the 1967 Outer Space Treaty (United Nations, 1984), space has now acquired non-negligible security and defense features. The Strategic Compass (Council of the European Union, 2022), document drafted by the European Council in March 2022, emphasizes the value of space for observation, surveillance, navigation, and communication and recognizes that these activities are now endangered by the irresponsible behavior of some actors in an increasingly congested and contested environment.

According to the United Nations Office for Outer Space (UNOOSA) (UNOOSA, 2023), the number of satellites brought to orbit has increased dramatically in recent years. At the time of writing, 8261 satellites are orbiting the earth, the majority of which are used for communications (Union of Concerned Scientists, 2023). This number is expected to double or even triple in the next years. UNOOSA has received over 2,000 satellite registrations in 2022 alone, and potentially 100,000 satellites could be launched over the next decade (UNOOSA, 2022). The use of space technology is no longer limited to governmental entities, and many new commercial operators have approached the sector. Satellites play a crucial role in various areas, such as communication, warning systems, broadcasting, meteorology, navigation, reconnaissance, remote sensing, and surveillance (Eshwari and Shrivastava, 2017). Their services impact nearly every sector, making any disruption to them potentially devastating (Pelton, 1994). Satellites are not only viewed as critical infrastructures by themselves but are behind the functioning of other critical infrastructures, representing a single point of failure for many sectors (Dacey, 2002).

Because of their complexity, space systems often lack high cybersecurity standards and a series of international policies to implement them (Varadharajan and Suri, 2022). Given the commercialization of

* Corresponding author.
E-mail addresses: francesco.casaril@imtlucca.it (F. Casaril), letterio.galletta@imtlucca.it (L. Galletta).

https://doi.org/10.1016/j.cose.2024.103799
Received 22 July 2023; Received in revised form 30 January 2024; Accepted 1 March 2024
Available online 8 March 2024
0167-4048/© 2024 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

space and the rearmament trends, malicious actors have found space infrastructure to be an attractive target. Therefore, it is necessary to enhance cybersecurity efforts for space infrastructures. Particular attention should be directed towards the security of the ground and user segments, as they have been identified as the most vulnerable elements susceptible to cyberattacks. When assessing the components comprising the infrastructure of the space industry, it is crucial to perceive space systems as cohesive and integral entities. As highlighted by Regulation (EU) 2021/696 of the European Parliament and of the Council, dated 28 April 2021, establishing the Union Space Programme and the European Union Agency for the Space Programme (EUSPA) (European Union, 2021), ensuring the security of all aspects of these systems is crucial for a sustainable space market. Launch capabilities, ground stations, and satellite manufacturing are fundamental components that demand special attention due to their critical roles within space systems. In alignment with the Space Strategy for Europe, the space industry should be regarded as an interconnected element within a broader system rather than existing in isolation from other industries. Consequently, the strategy emphasizes the need to consider space as an interoperable element within an extensive system. According to Article 34(1), the highest priority concerning security in the Space Program is safeguarding its infrastructure, encompassing both ground and space facilities, while ensuring the uninterrupted provision of services. This necessitates protection against physical and cyber threats alike.

Here, we focus on SatCom and, in particular, on the vulnerabilities that the interaction between the user segment and the ground stations can generate. These segments are often neglected and rarely considered when discussing space cybersecurity policies, and only a few studies assess the cyber vulnerabilities of the user segment. Given the complexity of space infrastructure, attacks on such components have to be considered preferable for attackers, as the attack cost is significantly reduced compared to other methods that aim at disrupting SatCom. In contrast, the results of such attacks could have the same disastrous impacts.

The advent of the so-called new space broadened the use and applications of space technologies such as SatCom (Kodheli et al., 2020); these domains, once reserved for a narrow audience, are expected to be widely employed by several users and even, as in the case of SatCom, to bridge the digital divide as much as concern access to the Internet. Studies in the field of SatCom cybersecurity exist, and vulnerabilities in the field have been discovered by researchers. However, the novelty brought by the new space paradigm (of which *IRIS*^{2} can be considered as an example) has not yet been extensively and deeply considered by researchers in terms of cybersecurity. Considering the actual state of space infrastructure, an assessment of what should be improved in cybersecurity is needed more than ever to build a resilient future constellation. When focusing on the specific user segment, current literature is outdated or lacks a comprehensive view of different products. Moreover, little consideration has been made toward understanding if existing standards and legal requirements currently meet the threats out there.

With this in mind, this paper aims to clearly define threats, understand how they affect these systems, and propagate to others (as shown in the case study). Then, we analyze how many such threats appear in vulnerable modems in the wild, and start mapping laws and standards in the field through a comparative approach, considering the development of *IRIS*^{2} constellation as background.

More precisely, this paper addresses the following research questions:

- RQ1: What are the most common vulnerabilities to ground and user segments in SatCom, and what are the vulnerabilities in the field?
- RQ2: What is the State of the Art of European and American standards and regulations in the field of space cybersecurity?
- RQ3: What are the best practices that stakeholders and entities involved in the management and operation of SatCom networks can use? Why are these practices not implemented?

We aim to provide valuable insights into this crucial subject by drawing on existing literature and case studies. More precisely, to address RQ1 the paper identifies the key cyber risks related to ground stations and user segments, with a special focus on satellite modem vulnerabilities, including unauthorized access, denial of service attacks, data breaches, and supply chain vulnerabilities. As a case study, the paper analyzes the Viasat cyberattack carried out in February 2022 (Viasat News Blog, 2022). Moreover, we use the Shodan search engine to investigate the exposure of satellite modems and other components of satellite networks on the Internet. To answer RQ2, we present and analyze guidelines and technical recommendations in the field of SatCom security defined by American and European stakeholders. Then, we present a comprehensive outline of the most effective practices for cyber risk management to address RQ3. These encompass the implementation of technical controls, such as access controls, network segmentation, and encryption, and the development of robust policies, procedures, and guidelines tailored to managing cyber risks. The paper also highlights the importance of continuous monitoring and incident response to detect and react to cyber incidents. Finally, the paper concludes with a discussion of future research directions and emerging trends. It should be noted that, despite the focus of the research being SatCom, the same considerations could be applied to different kinds of space infrastructures such as Global navigation satellite system (Kaplan and Hegarty, 2017) (GNSS) and Earth Observation (Lautenbacher, 2006) (EO) infrastructures. Our research relies on a specific case study, as obtaining real-world scenarios and empirical data on cyber incidents in the field can be extremely difficult due to underreporting by targeted organizations that prefer not to disclose cyber incidents and their consequences, especially due to the current geopolitical scenarios. We aim to address this limitation in future research.

The rest of the paper is organized as follows. In Section 2, we present an overview of SatCom describing its architecture, its main components, user and ground segments, and technology which is typical of this context. Section 3 presents the study of the Viasat attack describing the vulnerabilities used by the attackers and the consequence of the attack. In Section 4, we provide a general overview of the common vulnerabilities and mitigations in SatCom, focusing on user terminals. In Section 5, we present the results of our Shodan research about satellite network components that are accessible through the Internet and that have vulnerabilities. Section 6 presents and analyzes guidelines and technical recommendations in the field of SatCom security defined by American and European stakeholders. In Section 7 we discuss some lessons learned and best practices that all the actors involved in managing, administering, and functioning space infrastructure should implement. Finally, Section 8 compares our work with the relevant literature, and Section 9 draws some conclusions illustrating possible future research directions.

2. An overview of SatCom technology

SatCom could be defined as the technology that utilizes communication satellites orbiting around the Earth to transmit information, messages, voice, video, and digital data from one point to another. The communication satellites act as relays that receive signals from the Earth's terrestrial equipment, including fixed, mobile, and transportable terminals, and re-transmit them back to the receiving station on Earth without the need for physical cables or infrastructure (Kolawole, 2017). Here, we mainly focus on SatCom as this technology is crucial to the world's telecommunications infrastructure. Indeed, it represents most of today's satellite infrastructures, and its application ranges in various fields during the past 50 years, including radio broadcasting, weather forecasting, military, and government communications. While ground communication systems have received the majority of attention from academia and industry in recent years, corporate endeavors by top technology companies like SpaceX, Google, and Amazon have reignited interest in satellite-based systems. In particular, satellites are being used

to deliver services in a range of new application domains, e.g., to reach remote areas with unparalleled connectivity (in terms of bandwidth and cost) or to support Internet of Things (IoT) devices with low power requirements (Qu et al., 2017). Thus, recent commercial actions unmistakably point to SatCom as one of the most significant enabling technologies for aiding the construction of the impending sixth-generation (6G) networks (Saeed et al., 2021). It thus appears to have a promising future based on its business-related driving forces. According to a specialized study report by Market Research Future (MRFR), the SatCom market will reach USD 41,860 Million by 2025 with an 8.40% Compound Annual Growth Rate (CAGR) (Akre, 2022).

2.1. SatCom *architecture*

A SatCom system's communication architecture can be divided into three main components (see Fig. 1): the *space segment*, the *ground segment*, and the *user segment*. The space segment includes the *Satellite to Satellite* (SS) and the *Satellite to Ground* (SG) links. It can comprise *Geostationary Equatorial Orbit* (GEO), *Medium Earth Orbit* (MEO), and *Low Earth Orbit* (LEO) satellites deployed for various applications such as navigation, data connectivity, television broadcasting, radio broadcasting, imaging, and broadband Internet. Moreover, SatCom technologies are often used in military and defense communication systems. The main difference between military and commercial can be observed in the orbits and frequencies.

The most commonly used frequency bands for SatCom include L-band (1-2 GHz), C-band (4-8 GHz), Ku-band (12-18 GHz), Ka-band (26.5-40 GHz), and Q/V-band (30/40-50 GHz). L-band is commonly used for satellite phone and low data rate communication, while C-band is used for satellite TV broadcasting and government/military communication. Ku-band is used for high-speed Internet and satellite TV broadcasting, while Ka-band is used for high-speed Internet and military communication. Q/V-band is a relatively new frequency and is under test for future satellite communication systems. The choice of frequency depends on factors such as signal propagation, available bandwidth, and regulatory restrictions. The above-mentioned details are crucial when considering SatCom cybersecurity, as satellite radio frequencies can be affected by various cybersecurity risks, including intentional jamming, eavesdropping, data injection, and spoofing (Tedeschi et al., 2022). In the case of jamming, an attacker transmits a signal to interfere with the communication between the satellite and the ground station. In contrast, eavesdropping involves attackers intercepting the data transmitted between the satellite and the ground station. Data injection attacks can also occur when attackers send false data to the satellite, causing it to behave unexpectedly. Lastly, another cybersecurity risk that affects satellite radio frequencies is spoofing. Spoofing refers to transmitting fake signals that mimic legitimate signals to deceive the receiver. This can lead to the unauthorized access of satellite communication and the manipulation or destruction of satellite data. Spoofing can also be used to create false images or maps, which can mislead military and civilian decision-makers (Giray, 2013). It is a difficult attack to detect and defend against, as the spoofed signal can closely resemble a genuine signal. The consequences of successful spoofing attacks can be severe, especially in the case of critical satellite systems such as those used in military operations or emergency response situations. However, here we do not consider satellite radio frequency vulnerabilities. We refer the interested reader to the large literature on this topic (Wu et al., 2020). To understand the importance of a cyber-secure ground infrastructure is thus necessary to analyze the architecture of this component.

2.2. *The ground segment*

The ground segment enables communication between the satellites and user terminals. It includes dedicated Gateway stations, namely Satellite Operator, infrastructures for control, and Network Operator,

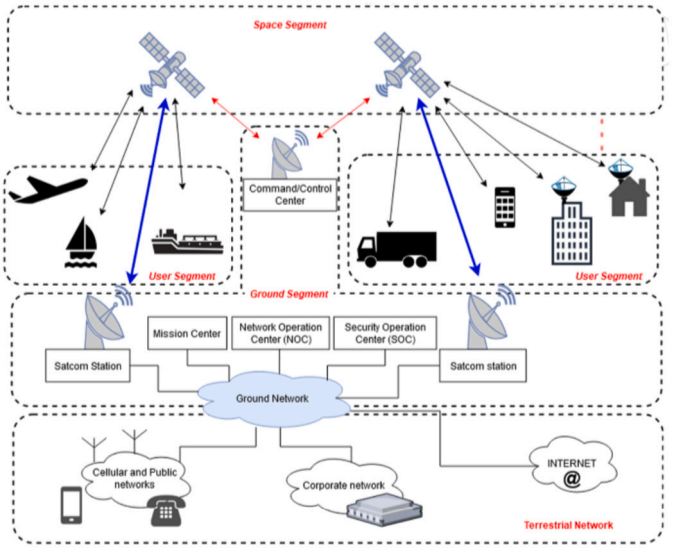

Fig. 1. SatCom Architecture.

such as the Network Control Centre (NCC), and the Network Management Centre (NMC) supporting the satellite access requests from users. Satellite ground systems and receivers comprise several components: the earth terminals and user receivers convert the satellite signal into useful data for the user devices, such as modems, antennas, and mobile phones. The ground segment contains the command and control system used to maintain the satellites' functionality and, in some cases, can also include the launch segment. To manage LEO and MEO satellite constellations, numerous ground stations are required across the planet to guarantee the communications between satellites and users (PwC, 2020). A standard ground station requires various infrastructures and activities to ensure smooth operations, which can be represented using a simplified value chain. The ground station value chain refers to the sequence of interconnected activities and processes involved in the operation of ground-based infrastructure in satellite communication systems. It encompasses the entire lifecycle of ground station operations, from initial setup and infrastructure development to data reception, processing, and utilization.

The ground station value chain involves various stakeholders, including satellite operators, ground station operators, equipment manufacturers, and service providers. It encompasses a range of activities, including the construction and maintenance of ground stations, deployment and alignment of antennas, signal reception and demodulation, data processing and analysis, and the provision of value-added services based on the received data. This value chain, known as the Ground Segment value chain, comprises three primary blocks: upstream, midstream, and downstream.

The three blocks of the Ground Segment value chain are further detailed as follows (PwC, 2020):

- The upstream block includes all the necessary hardware and software that facilitate mission operations, such as antennas, modems, and radio equipment, the launch facility, and the ground networks that provide connectivity among all the ground segment elements.
- The midstream block comprises all activities that support mission operations. It comprehends the control center and the IT facility, performing spacecraft and payload Telemetry Tracking and Control, downlinking signals, and retrieving data.
- The downstream block includes all activities performed once the data is retrieved on Earth. This includes data storage, preprocessing, such as error corrections and timestamps, and services based on data analytics.

The Ground Segment can be further divided into two main categories (Zhan et al., 2020): Ground stations for Tracking, Telemetry, and Control (TTC) and Communications Ground Stations (CGS). TTC is crucial in maintaining satellites' proper orbits and monitoring their performance. Whereas communications ground stations are responsible for processing and transmitting various types of data, such as imagery and voice, and often serve as a link to terrestrial networks. However, it is important to note that in most cases, the ground-based terrestrial network interconnections communicate with the communications ground station and not directly with the satellite.

2.3. The user segment

The second key element of SatCom infrastructure is the user segment. Apart from communications ground stations, numerous commercial user terminals on the market can receive data downlinks and even transmit data uplinks in some cases. For instance, GPS navigation devices often found in cars and satellite TV dishes are examples of downlink-only user terminals. In this last category, we also include other types of equipment such as Very Small Aperture Terminals (VSAT) (Comsys, 2010) and a new generation of user terminals, of which Starlink dishes (Yadav et al., 2022) are one of the most famous examples at the moment. The cybersecurity of these components that are often closer to the end-users is the focus of this research.

ETSI's Broadband Satellite Multimedia Working Group specified a reference architecture for IP-based satellite networks (ETSI, 2024). However, since we focus on the user segment, we can describe the architecture of such a segment as organized into three main layers: the *Access Layer*, the *Distribution Layer*, and the *Core Layer*. The Access Layer connects end-user devices, such as satellite terminals and modems, to the network and provides the physical and logical interface between the user equipment and the Distribution Layer. It may sometimes include additional equipment, such as amplifiers and filters, to optimize the signal quality and reliability.

The Distribution Layer is responsible for aggregating traffic data from the Access Layer and forwarding it to the Core Layer. It may include routers, switches, and other devices providing connectivity and managing network traffic. This layer also provides security and Quality of Service (QoS) features to ensure that traffic is prioritized and routed efficiently.

Lastly, the Core Layer transports traffic between different sites and networks. It provides high-bandwidth connectivity and may use technologies such as *Multiprotocol Label Switching* (MPLS) (Donner et al., 2004) and *Virtual Private Networks* (VPNs) to optimize traffic flow and ensure security. The Core Layer also includes network management systems and other tools for monitoring and controlling network performances.

The SatCom user segment infrastructure generally consists of various components that enable communication between the end-user and the satellite. These components include:

- Antennas (Correia et al., 2022): An antenna is used to transmit and receive signals to and from the satellite. The antenna must be designed to operate at the satellite signal frequency and accurately pointed toward the satellite for optimal communication.
- Modems (Heissler et al., 2005): A modem modulates and demodulates the satellite signal, and it is responsible for converting the digital signal from the user's device into an analog signal that can be transmitted over the satellite and vice versa.
- Routers (Wysocarski et al., 2007): In a satellite communication network, routers manage data flow between different devices and networks and connect user terminals, such as modems or other devices, to the satellite network. They can also connect different networks, such as Local Area Networks (LANs) or Wide Area Networks (WANs), to the satellite network.
- Transceivers (Kuang et al., 2017): A transceiver combines a transmitter and a receiver into a single unit and is used to transmit and receive signals over the satellite.
- Amplifiers (Calcutt and Tetley, 1994): An amplifier boosts the strength of the transmitted signal. This component is necessary to ensure the signal is strong enough to travel long distances and penetrate through obstacles.
- Terminals (Calcutt and Tetley, 1994): A terminal is the user's device connected to the SatCom system. It could be a laptop, phone, or any device capable of sending and receiving digital signals.
- User Management Systems (Mitra, 2005): A user management system manages the system's users, taking care of authentication, authorization, and accounting of users.
- Operations Support Systems (Debruin, 2008): An operations support system monitors the system's performance, identifying and resolving any issues that may arise and ensuring that the system operates at maximum efficiency.

These components work together to provide reliable and efficient communication between the user and the satellite. They may be integrated into the same hardware, depending on the product. As mentioned above, the user segment includes terminals such as satellite mobile phones, ships, and airplanes. These devices can communicate with satellites via the link between the ground segment and the user segment, such as the forward link, whereas they can use any communication technology to interact with the gateways. The forward link consists of an uplink (base station to satellite) and a downlink (satellite to mobile user). Some constellations like Iridium, Globalstar, Thuraya, and Inmarsat (Chini et al., 2010) allow a direct connection of the user handsets to the satellites using the User to Satellite (US) link that typically uses frequencies in the L-band (Chini et al., 2010).

For this research, one of the main components to be considered is the satellite modem, which converts digital signals from a computer or another device into analog signals that can be transmitted via satellite, and vice versa. Satellite modem communication protocols are the standards and rules that govern the communication between the antenna and the satellite modem and between the modem and the Ground Station Network. Several protocols exist, the most common include (Shah et al., 2014):

- Ethernet (Lee, 2011): It is a standard communication protocol to communicate over a cabled network. In SatCom, it allows communication between the satellite modem and other devices, such as routers or switches.
- TCP/IP (Ivancic et al., 2000): They are standard protocols for exchanging data over the Internet. In SatCom, they are commonly used to enable communication between the satellite modem and ground-based networks or devices.
- Simple Network Management Protocol (SNMP) (McLaughlin, 2011): It is a standard protocol to manage and monitor network devices. In SatCom systems, it is often used to monitor the performance of the satellite modem and other network devices.
- Telnet (Criscuolo et al., 2001): It is a standard protocol to establish a remote terminal connection between a client and a server. In SatCom, remote users can access ground-based equipment and services.
- Secure Shell Protocol (SSH) (Finch et al., 2012): Like Telnet, SSH provides a terminal connection between a client and a server. However, unlike Telnet, SSH uses encryption and authentication to secure the connection and protect against unauthorized access and data interception.
- TR-069 Protocol (Viasat News Blog, 2022): Several SatCom modems use it to manage and control remote terminals. It allows automatic configuration and management of devices, firmware upgrades, and fault diagnosis. The protocol also enables communication between

the modem and a remote management system, enabling centralized control and monitoring of the modem's performance.

The protocols above are the most common ones that may be used in SatCom modems and routers. Actually, the specific protocols used can vary depending on the specific system and application. Additionally, some proprietary protocols may be used for controlling the satellite modem and antenna, such as the iDirect protocol used by iDirect modems (Jegham et al., 2008) or OpenAMIP, an IP-based protocol that facilitates the exchange of information between an Antenna Controller Unit and a satellite (Gopal et al., 2022). Other key components that are often integrated into this complex infrastructure are VPN appliances that are commonly used in the ground infrastructure to connect remote users to the network securely. These appliances are designed to provide high levels of security and reliability, but, as discussed in the following section, they are not immune to cyber-attacks.

Finally, it should be considered that attacks can be launched in any of the segments mentioned above. In light of this, the user and ground segment should be properly guarded, and all communications coming from the satellite should be kept secure, regardless of its location.

3. From theory to practice: the attack to Viasat

3.1. Chronology of the attack

On February 24th, 2022, the satellite communication service provider Viasat experienced an outage of its KA-SAT Network due to a malware wiper attack that disabled thousands of end-user terminals (Viasat News Blog, 2022). According to a press release published by the same Viasat, the attack was not addressed to the KA-SAT satellite, but to a "*consumer-oriented partition of the KA-SAT network*" (Viasat News Blog, 2022), namely, Internet modems Tooway, SurfBeam2, SurfBeam2+. The attack, however, was not limited to Ukraine and had severe consequences on users, causing ripple effects across Europe. Indeed, not only thousands of customers in Ukraine, including the Ukrainian Government, army, and security services, were impacted, but also tens of thousands of users of other satellite broadband services suffered outages. In France, around 9,000 subscribers of the satellite broadband service NordNet's (ConnexionFrance, 2022) were affected, as well as almost 15.000 subscribers of the British broadband provider BigBlu (Techq, 2022) were impacted in Germany, France, Hungary, Greece, Italy, and Poland. The attack also damaged the German energy company Enercon (ENERCON, 2022), as remote monitoring and control access to its 5,800 wind turbines became unavailable due to its SCADA system relying on the KA-SAT network. Some satellite modems became unusable without the possibility of being repaired or updated remotely, resulting in thousands of customers being left without an Internet connection for weeks (Reversemode, 2022). Weeks later, Enercon stated that there were "difficulties with the availability of the hardware" with the supplier of the modems (ENERCON, 2022). According to Viasat, the attacker did not access end-user data and devices such as computers or mobile phones, and the KA-SAT satellite and its ground stations were not compromised, damaged, or involved in the attack. Interestingly, this part of the network is owned by the U.S. company Viasat but operated by Eutelsat's subsidiary Skylogic. In particular, the attack appears to have taken place in two main phases (Reversemode, 2022):

- A Denial-of-Service (DoS) attack was carried out on the Viasat Internet modems located mostly in Ukraine and Germany. Attackers exploited a vulnerability in the authentication mechanism of modems, enabling them to gain unauthorized access to the infrastructure's ground and user segments. This attack disrupted satellite communication services, requiring several days to restore them fully.
- Attackers exploited a vulnerability in the VPN appliances of Skylogic, which seems to be Fortigate's (Reversemode, 2022), an American multinational corporation that develops and sells cybersecurity solutions. They entered the ground network management segment of Viasat's KA-SAT network and gained control through a lateral movement. Once into the management section, attackers executed a series of commands uploading a wiper malware in the network and erasing the hard drive of ViaSat modems.

The attack targeted the satellite communication infrastructure's ground and user segment, affecting more than 15,000 users, including government agencies and military organizations, resulting in many users being unable to connect to the network. The alteration of the Viasat system certainly caused considerable difficulties for the Ukrainian military and government in the first hours of the conflict (Boschetti et al., 2022). However, the effect on the course of the conflict is difficult to estimate. In particular, since radio signals were jammed during the first phase of the invasion, the Ukrainian military relied on satellite communications to coordinate its troops. Soldiers were thus unable to use radios, and SatCom was considered a valuable alternative to communicate along the chain of command. Once this infrastructure was compromised, operations coordination became slower and more uncoordinated (Boschetti et al., 2022).

3.2. Analysis of the attack

The two-phase attack seemed to have been caused by vulnerabilities in the Internet modems and the VPN appliances. On one side, the DoS attack was caused by a "*misconfiguration in the management section of the satellite network*" (Reuters, 2022). It is suspected that the attackers were able to gain unauthorized access to a Ground Station, particularly the 'Element Management' section, which is synchronized across multiple gateways. They likely exploited a legitimate control protocol (Satellite Today, 2013), such as TR-069, that seems to have been employed by Viasat, to issue a command to deliver a malicious firmware update to the terminals. One possible method for carrying out this attack is using VLAN-based attacks. However, the entity managing this *management section* has not been disclosed, as well as what exactly this management section is. Some security analysts proposed that the Viasat SurfBeam Internet modems were probably configured through the TR-069 protocol, and an unpatched vulnerability in this protocol could have allowed hackers to perform the DoS attack (Reversemode, 2022). According to security researcher Ruben Santamarta, the TR069 'APP INSTALL' feature could have been the way through which hackers wiped the modems (Reversemode, 2022). Through this feature, attackers implemented functionalities that enabled the access control system to install arbitrary binaries on the modem without requiring signature verification or a complete firmware upgrade (Reversemode, 2022). The TR-096 protocol is often used to manage Customer Premises Equipment (CPE) devices such as routers, modems, and gateways. In the case of Viasat however, it is unclear the vulnerabilities that were exploited.

On the other side, the second phase of the attack, which resulted in access to the management section, was carried out, probably exploiting already known vulnerabilities. It seems that Fortinet, the VPN appliances provider of Skylogic, has been affected by relevant data breaches (Boschetti et al., 2022). In November 2021, Fortinet learned that a malicious actor disclosed around 500.000 SSL-VPN access information from 87,000 FortiGate SSL-VPN devices. These credentials were obtained from systems that remained unpatched against FG-IR-18-384 / CVE-2018-13379 at the time of the actor's scan (Fortinet, 2021). This CVE, due to an Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in various Fortinet products (CVE, 2018) under SSL VPN web portal, allowed an unauthenticated attacker to download system files via specially crafted HTTP (Hypertext Transfer Protocol) resource requests. The credentials were leaked in two Russian-speaking forums, namely Groove and RAMP (BleepingComputer, 2021). In March 2021, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) observed Advanced Persistent Threat (APT) actors scanning devices on ports 4443, 8443,

and 10443 looking for CVE-2018-13379 and enumerating devices for CVE-2020-12812 and CVE-2019-5591 (FBI-CISA, 2021). Thus, already in 2019, these vulnerabilities were well known, and in 2021 the FBI and CISA warned about the malicious activity of hackers targeting these vulnerabilities in a Joint Cybersecurity Advisory. Even if Fortinet promptly patched them, neither Skylogic nor Viasat signaled them to their customers. The stolen credentials of these VPN appliances were thus probably the entry point of hackers in the network (Reversemode, 2022).

3.3. Lessons learned

Although all the details about the attack are still unclear, the incident presents a unique opportunity for the entire sector, both commercial and governmental, to acquire useful insights and learn how to avoid similar disruptions. The attack could be considered one of the most significant publicly known against a space system so far. Furthermore, as noted by Boschetti et al. (2022), the incident took place hours before the start of the Russian invasion of Ukraine in February 2022, indicating the potential utilization of a cyberattack as an initial act, having significant implications within a military context. Additionally, Viasat's dual-use paradigm, serving as both a commercial and military asset, adds complexity to the incident and indicates trends for future attacks as the space sector continues to commercialize.

The attack should be considered by European Stakeholders, especially in this historic moment since the European Union's decision to provide itself with a multi-orbit Satellite constellation for Communications, the *IRIS*^{2}. SatCom and GovSatCom, in particular, have demonstrated to be essential technologies to rely upon in critical scenarios such as conflicts, natural disasters, terroristic attacks, and in general, every time different means of communication are needed. The Viasat attack highlighted the need for a reliable SatCom infrastructure. Still, we should not take for granted that the issues raised by the attack will be transposed in future policies and guidelines. The attack demonstrated that commercial satellites are not as reliable as military ones, even if they are often used for the same purposes as in Ukraine. Given the vulnerability of commercial satellites, an attack against these constellations could potentially provoke more disastrous consequences than an attack on a military satellite infrastructure, where risk management and risk assessment policies are always well-defined and implemented. A clear vulnerability shown by the attack is the complexity of commercial space services. In the considered case, various companies were the owners and operators of the space, ground, and user segment and were distributed in different countries and thus under different jurisdictions. Moreover, the architecture of these systems includes different IT service providers such as Fortinet. This complexity implies different levels of not only vulnerabilities but also responsibilities regarding the security of the system. The Viasat case study shows how attackers can take advantage of trust relationships and access privileges between space companies and their IT subcontractors to gain access to networks: attackers exploited the connection between VPN provider and Skylogic, to gain access to Viasat's network.

It should be kept in mind that while regulatory compliance should serve as a baseline, relying solely on a compliance-focused security approach falls short due to minimum standards, outdated requirements, and a one-size-fits-all mentality. The SatCom sector, like many others, necessitates a comprehensive risk management strategy, evaluating risks from various sources. The evaluation of third-party cybersecurity risks, especially IT service providers and significant suppliers, is crucial before onboarding (Benaroch, 2020). Continuous security goes beyond initial assessments, requiring contractual obligations, ongoing monitoring, compliance management, and data use restrictions. What is needed in the industry is a shared security model that dispels the misconception that security is solely the responsibility of one of the parties involved in the architecture. The future of third-party risk management involves growing complexity, demanding automation, threat intelligence, and an always-on risk management mindset. Cyber Third Party Risk Management (C-TPRM) can involve both intrusive methods like penetration testing and non-intrusive methods that synthesize publicly available information (Keskin et al., 2021). While it is an emerging field, a range of methodologies is being explored to create an effective and efficient system for managing third-party cybersecurity risks (Rasner, 2021).

In conclusion, the primary focus of the attack analysis should be on the possible security vulnerabilities that can arise from the intricate wholesale operations involved in a satellite infrastructure. This complexity extends down the chain to ground station operators, satellite service providers, distributors, and resellers, all requiring some level of access to provide their services. It is exactly the integration of these various components that present the highest security challenges. This also raises legal concerns about the cybersecurity responsibilities and minimum requirements that providers must impose on their subcontractors. Commercial actors that decide to provide services to specific categories of users, such as governments and the military, should consider that their business could be significantly threatened, and their risk assessment and threat model should be reevaluated. All these considerations should translate into a higher budget dedicated to cybersecurity in cases of specific users. The concept of satellites as a single point of failure for multiple sectors is probably the most relevant issue highlighted by the attack. The propagation of the DoS to modems used in different sectors and countries showed the threat that a non-segmented network could provoke. Especially when designing *IRIS*^{2}, which will probably rely upon a mix of commercial already existent SatCom infrastructures and new ones, the EU stakeholders should reconsider the dual-use of these technologies. The non-separation will automatically lead to a higher likelihood of propagation in case of attacks. Even the distinction between military and civilian when discussing SatCom, but in general satellite infrastructures, should be considered outdated. Given the reliance of many ground-based critical infrastructures on space-based ones, not only for connectivity but also for synchronization, commercial space companies, in the case they are providing services to specific users, should grant the same security as military infrastructures and be audited in the same way. This is even more important considering the European tendency to foster the commercialization of space. In the case of Ukraine, the country relies totally on foreign space infrastructures for its military operations, this significantly reduced its capacity to implement military strategies autonomously. Various commercial satellite service providers, such as Starlink (Ray and Selvamurthy, 2023), Maxar (Bennett et al., 2022), and BlackSky (Hurova, 2022), allowed the country to use drones and collect intelligence for defense and attack campaigns. Nevertheless, it is advisable to exercise caution when assigning military capabilities to commercial operators, and this consideration should be extended to encompass all services that are in any way linked to civil security and defense.

4. SatCom user segment: vulnerabilities and mitigations

Information regarding the technical aspects of SatCom user segment vulnerabilities, breaches, and mitigation strategies for systems and networks are often unavailable. It appears that most of the industry and service providers have been reluctant to disclose technical details of security breaches to the public. This section aims to provide a general overview of all the common vulnerabilities in SatCom networks, particularly user terminals, and review mitigation techniques and strategies for their reduction.

4.1. Context

From the viewpoint of an attacker aiming to compromise satellite networks, the user segment represents a cost-efficient attack. As the ViaSat case demonstrated, the disruption caused by compromising a small portion of the network cannot be ignored. From the user segment, an attacker can move laterally in the network and maybe even take control of

the entire command-and-control system. This happened in the 90s when attackers acquired access to the flight control system of NASA's Goddard Space Flight Center (Fritz, 2013) and exposed the ROSAT telescope sensors to the sun, causing the inoperability of the satellite. In recent years however, with the increase of commercial ground stations and with the introduction of the concept of Ground Station as a Service (Boschetti et al., 2022), these kinds of attacks increased in their frequency and their complexity (Falco, 2018). To gain access to the component of a satellite or information about a company, attackers previously faced high barriers due to the complexity and cost. However, with the rise of new space companies, which are more communicative about their systems' supply chain, contracts, and employees, malicious actors may obtain critical information useful to support their malicious activities. Additionally, modern space systems increasingly rely on cheaper *Commercial Off-the-Shelf* (COTS) components and standardized hardware and software, making it easier for potential attackers to purchase and search for vulnerabilities. This also means that if a vulnerability is found in one COTS component, all satellites using that component are vulnerable. Ground stations are thus vulnerable to cyber-attacks, which could compromise the confidentiality, integrity, and availability of critical space-based systems and operations. On January 2023, the Chief of Space Operations, U.S. Space Force Gen. B. Chance Saltzman, speaking at the Air and Space Forces Association Board of Directors meeting in Arlington, VA, highlighted that "*Satellites in space are not useful if the linkages to them and the ground network that moves the information around what you get from satellites is not assured, is not capable, is not accessible. The cyber activity that has hurt satellite operations is a reminder that we should think about cyber protection of our ground networks* (Air and Space Forces, 2023)."

4.2. COTS components and their risks

In recent years, the increasing reliance on COTS components in satellite communication systems has raised cybersecurity concerns. While COTS components can offer cost savings and improved performance because of their wide availability on the market, their integration into SatCom systems creates a significant cybersecurity challenge. Since these components are not specifically designed for any particular application, they may not have undergone rigorous security testing and certification processes necessary for use in SatCom systems. A list of COTS typically used in SatCom networks follows:

- Modems: COTS modems are commonly used in SatCom systems, however, they can be vulnerable to attacks such as denial of service, unauthorized access, and data interception. For example, attackers can exploit software vulnerabilities in the modem's firmware to gain unauthorized access to the network or launch a DDoS attack by flooding the modem with traffic. Examples of these modems are: iDirect Evolution X7, Hughes HX200, Comtech EF Data CDM-625 Advanced Satellite Modem, ViaSat MD-1366/U Advanced Extremely High Frequency (AEHF) Satellite Modem, Newtec Dialog MDM6000, Advantech Wireless AMT-75 HT Satellite Modem, Gilat SkyEdge II-c, GRC RP-1G, SWE-DISH IPT Suitcase 1.3M Ku-Band Flyaway Terminal, Datum Systems M7S Modem, ND SatCom SKY-WAN 5G, Advantech Wireless AMT-83L High-Speed Satellite Modem.
- General Purpose Processors (GPPs): GPPs are often used in satellite payloads and ground stations to perform signal processing and data encryption tasks. However, these processors are not specifically designed for satellite applications and can be vulnerable to side-channel attacks. For example, an attacker could use a power analysis attack to extract sensitive information from a GPP by analyzing its power consumption. Examples of GPP used in Satellite Systems are: ARM-Cortex-M/R and other MMU-less devices.
- Operating Systems (OS): Common operating systems such as Windows and Linux are often used in SatCom systems due to their wide availability and versatility. However, these operating systems are not designed with satellite-specific security considerations and may contain vulnerabilities attackers can exploit. For example, an attacker could use a buffer overflow attack to exploit a vulnerability in the OS and gain unauthorized access to the system.
- Wireless Communications: SatCom systems rely on wireless communication links between satellites, ground stations, and user terminals. However, these wireless links are vulnerable to interception and interference by attackers. For example, an attacker could use a software-defined radio to intercept and decode the wireless communication signals or launch a jamming attack to disrupt the communication link.

The use of COTS components also poses supply chain risks. These components are often manufactured overseas, and the supply chain may not be secure. Attackers can exploit vulnerabilities in the supply chain to introduce malicious components into a system, compromising its security. Implementing robust security controls to mitigate the cybersecurity risks associated with COTS components is essential. These controls should include secure supply chain management, rigorous security testing, certification processes, continuous monitoring, and threat intelligence. The use of COTS components in critical SatCom systems should be limited. Government and commercial actors should prioritize using components that have undergone rigorous security testing and certification.

4.3. Common vulnerabilities and mitigations

The cybersecurity challenges faced by the SatCom user segment are relatively new but require comprehensive measures to ensure the integrity and confidentiality of communications. By understanding these vulnerabilities and implementing appropriate measures, organizations can enhance the security posture of their SatCom networks and protect against potential threats. To mitigate cyber risks, various strategies and technologies can be employed. Table 1 explores some of the most common vulnerabilities and attacks on SatCom systems and provides some guidelines on how to mitigate them. Although the table is non-exhaustive, it describes well how exposed SatCom systems are to cyber threats. The content of the Table 1 will be further explained in the following section.

In the last years, as costs reduced and attacks increased, several user terminals started being targeted, and vulnerabilities being actively exploited (Peeters, 2022). Table 2 on the other side provides some examples of vulnerabilities discovered in popular SatCom user terminals. Understanding these vulnerabilities is essential to develop effective cybersecurity strategies to protect satellite systems from potential cyber-attacks. Note that the list does not include all those vulnerabilities that affect the other components of the ground segment, such as switches, firewalls, and VPN appliances that are no less critical in the SatCom infrastructure.

Satellite communication networks are extremely vulnerable to attacks from adversaries who target satellite user terminals, as many lack the same protections commonly found in terrestrial modems/routers. As with any networked device, satellite modems are susceptible to cyberattacks. Cybercriminals can attempt to exploit vulnerabilities in the device's firmware or software to gain unauthorized access, intercept data, or for other malicious activities (see Table 2 for some examples). Satellite routers have been known to present an attack surface through their administrator interface and have been secured through better password protection and browser policies. However, as new satellite Internet providers become more prevalent, new routers are often designed without mitigations against vulnerabilities already common in terrestrial routers. Moreover, since the router is part of a physical system that often includes the antenna, securing the admin interface is of greater importance. Attacks on the admin interface can affect the an-

Table 1
Vulnerability/Attack and Mitigation.

Vulnerability/Attack	Common mitigations/recommendations
Lack of Encryption	• Use network encryption solutions, such as IPsec or TLS VPNs, to encrypt network communications over SAT links. • Apply mutually authenticated, encrypted TRANSEC down to the outermost vendor-proprietary transmission protocol. • Apply encryption down to and including the outermost vendor-proprietary transmission protocol. • Use point-to-point communications over IKE/IPsec-encrypted VPNs with strong authentication and key exchange methods.
Weak Authentication/Lack of Access Control	• Implement strong passwords and multi-factor authentication. • Employ RBAC and ABAC access controls. • Implement approved firewalls and network segmentation. • Change all default credentials. • Use intrusion detection and prevention systems. • Implement a need-to-know access policy.
Vulnerabilities in Software and Firmware	• Keep all IT equipment updated with the latest security patches. • Acquire updates and upgrades from trusted sources.
Cross-Site Scripting (XSS)	• Use input validation and output encoding to prevent XSS attacks. • Use Content Security Policy (CSP) to whitelist allowed sources of scripts and resources.
Brute-Force Attacks	• Implement rate limiting. • Use strong and unique passwords. • Encourage two-factor authentication. • Use CAPTCHA or similar techniques.
Jamming	• Employ frequency hopping techniques. • Use anti-jam antennas and polarization diversity. • Use commercial anti-jamming solutions.
Denial of Service (DoS)	• Employ intrusion detection and prevention systems. • Utilize commercial DoS protection solutions.
Malware and Virus	• Employ antivirus and antimalware solutions. • Use network segmentation.
Physical Threats	• Ensure physical security of SatCom equipment and facilities. • Use tamper-evident seals. • Implement security cameras and monitoring tools. • Use hardened and ruggedized equipment. • Use secure, tamper-evident containers for transportation.

Table 2
Examples of terminal vulnerabilities.

Terminal	CVE	Description
Starlink Satellite Modem	See reference (Smailes et al., 2023)	Fuzzing to uncover a denial-of-service attack on the Starlink user terminal
Newtec Dialog MDM6000	ZSL-2016-5359 (Zero Science Lab, 2016)	The terminal suffers from cross-site scripting vulnerability. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
Hughes Network Systems 9201, 9450, and 9502	CVE-2013-6035 (Ruben Santamarta, 2013)	The terminal does not require authentication for sessions on TCP port 1827, which allows remote attackers to execute arbitrary code via unspecified protocol operations.
NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite, (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106	CVE-2020-11549 (ModZero, 2020)	The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system.
Hughes Network Systems Router Terminal for HX200 v8.3.1.14, HX90 v6.11.0.5, HX50L v6.10.0.18, HN9460 v8.2.0.48, and HN7000S v6.9.0.37	CVE-2023-22971 (Zero Science Lab, 2023)	Cross-site scripting vulnerability in Hughes Network Systems Router Terminal allows unauthenticated attackers to misuse frames, include JS/HTML code and steal sensitive information from legitimate users of the application.

tenna's physical state, resulting in a denial of service and damage to the antenna's motors and other hardware through overuse.

In the context of router security, the TR-096 protocol is often used to manage Customer Premises Equipment (CPE) devices such as routers, modems, and gateways. Like any network protocol, it carries potential cybersecurity risks (Broad Band Forum, 2020), among which:

- Authentication vulnerabilities: The protocol authentication mechanisms may be susceptible to brute-force attacks or other forms of exploitation, which can allow unauthorized access to CPE devices.
- Malicious firmware updates: The TR-096 protocol allows to remotely update the firmware. Attackers can exploit this feature to upload malicious firmware to devices, which can be used to steal sensitive data or conduct other malicious activities.
- Network reconnaissance: The protocol allows retrieving device information, such as serial numbers, firmware versions, and hardware specifications. Attackers can use this information to conduct reconnaissance on the network and identify potential vulnerabilities.
- Denial-of-service attacks: The TR-096 protocol uses HTTP-based communication, which can be vulnerable to denial-of-service (DoS) attacks: attackers can flood the device with HTTP requests, which can overwhelm the device and render it unusable.
- Man-in-the-middle attacks: The TR-096 protocol does not provide end-to-end encryption and authentication, allowing attackers to in-

Table 3
A summary of the vulnerable devices found by Shodan.

IP	Device	Organization / ISP (Country)	Organization's Revenues ($)	Country/City	Vulnerabilities	Open Ports
82.***	N/A	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	CVE-2020-15778 - CVE-2021-36368	22, 161
161.***	N/A	INMARSAT GLOBAL LIMITED (UK)	1.2 B	7 United Kingdom Hounslow	CVE-2022-31813 - CVE-2020-1927 - CVE-2021-4044	21, 22, 23, 443
165.***	Router MikroTik	ViaSat, Inc./ViaSat, Inc. (USA)	2.78 B	Germany Frankfurt	CVE-2022-22707 - CVE-2019-11072 - CVE-2018-19052	161 - 9997, 10000
219.***	Server	COLT Technology Services Group Limited / Viasat SPA (UK)	1.2 B	Italy/Milan	CVE-2009-4444 - CVE-2009-2521 - CVE-2008-1446	21, 80
62.***	Newtec DVB-S L-band Satellite Modulator NTC/2180.xA	Satellite Mediaport Services Ltd. (UK)	>5 M	United Kingdom Rugby	N/A	80, 161
80.***	Newtec ntc7102	YAHSAT FRANKFURT (UAE)	206 M	Germany Oberasbach	N/A	80, 161
84.***	Comtech EF Data CDM-570L/IP L-Band Satellite Modem	IABG Teleport GmbH (DE)	265 M	Germany Munich	N/A	161
188.***	Gilat Modem	PRIVATE JOINT STOCK COMPANY DATAGROUP/SKYLOGIC S.P.A. (NA)	NA	Ukraine/Kyiv	CVE-2021-40438 - CVE-2022-37436	161
82.***	MikroTik Router	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	N/A	22, 23, 53, 80, 2000, 8291, 8728
82.***	N/A	Horizonsat FZ LLC (UAE)	6.2 M	Germany Niederdorla	CVE-2022-36760 CVE-2022-28615 CVE-2022-30556 CVE-2023-25690	22, 80, 443
78.***	Cisco ASR 1000 Series Aggregation Services Router	MPLS European Backbone 1 of Phibee-Telecom/Phibee Telecom SAS (FR)	>5 M	France/Paris	N/A	121, 161

tercept and manipulate traffic between the CPE device and the management server.

While these are potential risks, the actual exploitation will depend on the specific implementation and configuration of the TR-096 protocol within an organization's network. Proper security controls and risk assessments should be conducted to mitigate these risks.

5. Looking for unpatched satellite networks in the field

In this section, we perform an on-field investigation of vulnerabilities within satellite communication SatCom systems. We exploit the Shodan search engine (Fernández-Caramés and Fraga-Lamas, 2020) to investigate the exposure of satellite modems and other components of satellite networks on the Internet. Shodan is a powerful tool for exploring Internet-connected devices and their associated vulnerabilities. Shodan primarily focuses on network-level information and allows discovering devices with open ports, publicly accessible services, and exposed systems that may unintentionally disclose sensitive information or present potential security risks. By using several search terms, including the names of SatCom service providers and names of commonly used satellite modems, we identified several SatCom network devices that are accessible on the Internet and that are vulnerable.

We performed our research on Shodan according to the following methodology.

- We first consulted the websites of the major satellite modem manufacturers such as *Comtech* (Comtech, 2023a), *iDirect* (iDirect, 2023), *Hughes* (Hughes, 2023), and other databases containing technical specifications and listings of hardware.
- Then, we performed Shodan queries containing both the models of the modems and the names of the ISPs or operators that may manage the infrastructure.
- By using specific keywords related to European Satcom service providers, such as "Intelsat", "Eutelsat", "Iridium", "Viasat", "IABG", "Inmarsat" and others, along with popular satellite modem names like "iDirect", "Comtech", "Hughes" and "Cobham", we looked for potential vulnerabilities and we assessed the risks associated with the exposed devices.

We have narrowed the scope of research to equipment located in Europe and mainly in the Member States of the Union. This is because the research aims at identifying SatCom service providers that may fall under the framework of European legislation such as NIS2 Directive. However, as highlighted by the Viasat case study, the attack on a piece of infrastructure outside the European Union's borders can have consequences on Member States, their economies, and security. Moreover, despite these devices being located in Europe, some of the ISPs that manage them are in countries such as the UAE or the USA. This complicates the enforcement of European standards and monitoring mechanisms as well as weakens the application of fines in case of non-compliance with European laws.

We collected data about open ports, ISP information, device characteristics, and approximate location from Shodan's results. We organized the data in a tabular format to clearly overview the findings. The tabular representation allows for easy analysis and identification of potential security risks of the exposed and unpatched satellite modems. Indeed, by the open ports and signaled vulnerabilities, it is possible to assess the level of risk posed by each device and determine the potential impact on SatCom users and industries. Identifying the device type was not always possible solely based on the collected data. However, we tried to categorize the devices whenever feasible by examining factors such as open ports, response banners, and known vulnerabilities.

A short summary of the results of our Shodan search is Table 3. The results reveal the presence of several satellite modems with unpatched vulnerabilities used by different ISPs. Our results also reflect the diver-

sity of satellite communication infrastructure and the many vendors and technologies involved. Each found device may have unique characteristics and vulnerabilities, and various ISPs may have different approaches to managing and securing their infrastructure. Understanding this diversity is essential for implementing comprehensive security measures for specific risks and challenges associated with different devices and ISPs. Table 3 provides a non-exhaustive list of the vulnerabilities that affect the identified hardware. The vulnerabilities with the highest score are:

- CVE-2023-25690 (Apache Software Foundation, 2023): Certain configurations of the Apache HTTP Server from versions 2.4.0 through 2.4.55 may be vulnerable to HTTP Request Smuggling, a technique for interfering with the way a web application processes sequences of HTTP requests that are received from one or more users. The vulnerability occurs when the proxy module is enabled with certain RewriteRule or ProxyPassMatch directives. These directives involve matching and inserting user-supplied data into the proxied request using variable substitution. Exploiting this vulnerability, an attacker can split or smuggle requests, potentially bypassing access controls on the proxy server, inadvertently proxying unintended URLs to legitimate origin servers, and even poisoning the cache.
- CVE-2020-15778 (NIST, 2020a): the `scp` utility in OpenSSH version 8.3p1 is vulnerable to a command injection. It allows for the execution of arbitrary commands by exploiting backtick characters in the input concerning the destination address. It is important to note that this vulnerability is labeled as *DISPUTED* because the vendor has reportedly stated that they intentionally omit validation of "anomalous argument transfers" to avoid breaking existing workflows.
- CVE-2022-31813 (NIST, 2022): This vulnerability is in the web-based management interface of Cisco IOS XE Software and could allow an unauthenticated, remote attacker with read-only privileges to execute arbitrary code with root privileges on an affected device.

The presence of multiple CVEs emphasizes the need for continuous monitoring, prompt remediation, and ongoing security measures to protect satellite communication and the connected infrastructure. Using such information on the vulnerabilities of each device, stakeholders can prioritize their efforts and try to introduce mitigations to protect their devices. This includes implementing regular patching and firmware updates, conducting security assessments and audits, enforcing secure configuration practices, and promoting security awareness and training among users and operators.

Our results show only a partial view of devices open to potential threats, as many other modems from other SatCom service providers may be as well on the list. The NIS2 Directive will oblige these actors to report cyber incidents and prepare business risk management strategies. However, at the moment, even if issues relating to vulnerability and patch management have been recognized as the basis for liability (Kitchen et al., 2021), according to standards such as ISO/IEC 27002:2022 (Iso/iec, 2022), in Europe as in many other countries no explicit legal obligations exist for companies to patch their products (Maurushat and Nguyen, 2022). This may cause European stakeholders to underestimate the potential impact of an attack on these networks on national security. Moreover, according to the Critical Entities Resilience directive (European Parliament and Council, 2022) (CER), modems and routers that are not industrial, such as the ones used by many satellite services providers, are class I products that pose minimal security risks. However, as seen in this paper, a lateral movement that starts with an attack on these modems may generate a non-neglectable security incident.

Based on these findings, future work could be carried out by performing a detailed vulnerability assessment of the devices identified and evaluating the potential risks that attacks such as lateral movements can have on the identified infrastructures.

6. Build cybersecure space links: the US and EU approaches

Operating a satellite is increasingly similar to administrating a computer network, as SatCom often relies on IP-based space links. However, unlike servers, IP-based space systems have their "wires" open to the public. This means that space systems, as listed above, have to deal with a very broad spectrum of threats, from low sophistication as DoS/Jamming to sophisticated root access gain attempts. For these reasons, cybersecurity must be perceived as a must during the lifecycle of space systems development. This requires a cultural shift for space companies. A holistic approach is needed to consider confidentiality, authentication, data integrity, and availability. The United States and, to a certain extent, the EU are moving in this direction, designing policies and recommendations to face the threats mentioned above. The following section analyzes some guidelines and technical recommendations defined by American and European stakeholders.

6.1. *The NSA guidelines on* SatCom

According to a cybersecurity advisory published by the United States National Security Agency (NSA) in June 2022 (NSA, 2022a), the majority of the SatCom systems that include terminals, modems, and ground stations should be considered as unencrypted wireless networks, given their widespread lack of encryption. These systems should not be relied upon even if they offer virtual network separation capabilities because, in most cases, they do not provide access control, separation, or confidentiality of sensitive information as the devices mentioned in Table 2. The fact that these networks can be connected to the Internet makes them easily targetable for remote attacks and exploitation. In the US, controlled unclassified information (CUI) must be encrypted at least with commercial network encryption solutions, including Internet Protocol Security (IPsec) or Transport Layer Security Virtual Private Networks (TLS VPNs) (CNSSP 15, 2016). To enhance the security of network infrastructures, the US National Security Agency advises using encrypted services and recommends disabling all clear text administration services such as Telnet, HTTP, FTP (File Transfer Protocol), and SNMP (Simple Network Management Protocol) version 1/2. This measure helps prevent adversaries from easily accessing sensitive information by intercepting network traffic (NSA, 2022b). Administration services should be configured to use up-to-date protocols and have adequate security settings enabled. For remote access to devices, SSH version 2 is the recommended method. Additionally, HTTPS servers should be configured to accept only Transport Layer Security (TLS) version 1.2 or higher to ensure encryption.

As for encryption, the National Institute of Standards and Technology (NIST) released the guidelines SP 800-131A rev2 (NIST, 2019) and SP 800-56A rev3 (NIST, 2020b) for the use of cryptographic algorithms and the choice of key lengths. These guidelines recommend that point-to-point communications over IP-based networks should use IKE/IPsec-encrypted VPNs with certificates or pre-shared keys for peer authentication and a Diffie-Hellman (DH) key exchange of at least 3072 bits or Elliptic Curve DH (ECDH) keys of 384 bits or larger (groups 14, 15, 16, 19, or 20). In the US, point-to-point communications should conform to CNSSP 15 standards (CNSSP 15, 2016) for National Security Systems (NSS). The CNSSP 15 is the policy regulating commercial cryptographic algorithms' usage for NSS. It is updated periodically to incorporate the latest standards and processes from CNSS and NSA. As of September 2022 (Ver. 1.0), the current version specifies the CNSA Suite 1.0, and will soon be updated to include the CNSA Suite 2.0 and Quantum Computing algorithms (Corcoran and Jenkins, 2022). The CNSA Suite 2.0 is detailed in Table 4.

As much as concerns key exchange, the NSA recommends avoiding aggressive mode and using IPsec VPNs to provide mutual authentication to both ends and secure the data in transit. TLS-based VPNs should use similar cryptographic algorithms as the ones in Table 4, and multi-point encrypted VPNs can be used in architectures where many point-to-point

Table 4
CNSA Suite 2.0 Cryptographic Algorithms.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197 (FIPS, 2001)	Use 256-bit keys for all classification levels.
CRYSTALLS-Kyber	Asymmetric algorithm for key establishment	-	Use Level V for all classification levels.
CRYSTALLS-Dilithium	Asymmetric algorithm for digital signatures	-	Use Level V for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for compute digests for information	FIPS PUB 180-4 (FIPS, 2015)	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208 (Cooper et al., 2020)	All parameters approved for all classification levels. SHA-256/192 is recommended.
Extended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software.	NIST SP 800-208 (Cooper et al., 2020)	All parameters approved for all classification levels.

VPNs are unmanageable (Korhonen, 2019). The NSA advises using mutually authenticated, encrypted TRANSEC where encryption is applied to the outermost transmission protocol using an approved pseudorandom keystream (AES 256) and key management scheme. Moreover, when using commercial satellite communications for mobile devices, best practice guidance suggests avoiding descriptive naming conventions and identifiers in device configurations to prevent external actors from easily identifying the devices and understanding their purposes.

Regarding procurement, in May 2022, the Space System Command of the United States approved the Infrastructure Asset Pre-Approval (IA-Pre) Initiative (Space Systems Command, 2022) in collaboration with the Commercial Services Office (CSCO). The initiative aims to enhance cybersecurity to reinforce CSCO's service evaluations and procurements for the Department of Defense (DoD). The CSCO started accepting IA-Pre applications for a restricted number of assets to perform assessments. The new initiative will replace the outdated self-assessment process where commercial companies submit their system information through a questionnaire, and CSCO evaluates it during acquisition. IA-Pre emphasizes on-site assessments for cybersecurity compliance verification by third-party assessors authorized by the U.S. Space Force Security Controls Assessor (SCA). The program also focuses on effective safeguards application and validation and weak point mitigation to decrease cybersecurity risks that may affect DoD missions that depend on CSCO for services. In the first phase, the US Space Force Authorizing Official will evaluate the cybersecurity assessments of the companies for approval as the industry progresses through the IA-Pre program. Afterward, CSCO will put the industry partner and the evaluated assets on an approved platform list. The industry partner will no longer require a cybersecurity evaluation before being awarded a contract for covered assets. IA-Pre trials started in June 2022.

This framework, however, is applied only to those operators that collaborate with the DoD. For commercial satellite operators not involved in defense initiatives, the regulatory framework is less stringent. One of the regulatory standards that could apply to these circumstances is the NISTIR 8270 (Scholl and Suloway, 2022). The document briefly introduces cybersecurity risk management for the commercial satellite industry to start managing cybersecurity risks in space. Developing a Cybersecurity Framework was a response to Executive Order 13636 (CFR13636, 2013), which aims to enhance the cybersecurity of critical infrastructures. It defines a Cybersecurity Framework (CSF) that adopts a risk management approach to cybersecurity and can be customized for different industries. It offers standardized terminology and methodology that organizations can implement based on their resources and operational requirements. The CSF comprises five functions: identify, protect, detect, respond, and recover. It is presented in a circular format to emphasize that cybersecurity is a continuous process that enables organizations to adapt to evolving cyber threats.

The NISTIR 8270 discusses the importance of creating and maintaining a cybersecurity program for space operations. The CSF helps to implement a cybersecurity program through seven steps effectively (Scholl and Suloway, 2022):

- Step 1: Establish the scope and priorities of the program. This step is critical to address cybersecurity in the earliest stages of building the components of the space architecture and embedding risk-reducing measures that meet the organizational mission and business objectives into the design and supply chain.
- Step 2: Drive the organization to related systems, assets, regulatory requirements, and its overall risk approach. The organization then works to identify threats and vulnerabilities applicable to those systems and assets.
- Step 3: Create a profile to understand the organization's current cybersecurity posture. An assessment of how the CSF functions are being implemented within the organization is created by listing the subcategory activities that are currently being implemented.
- Step 4:Conduct a risk assessment, where the organization analyzes the operational environment, identifies emerging risks, and uses cyber threat information from internal and external sources to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.
- Step 5: Create a target profile by selecting the subcategories that support the organization's desired cybersecurity outcomes.
- Step 6: Determine, analyze, and prioritize gaps. The organization compares the current and target profiles to identify potential gaps. When paired with a threat, a risk assessment can be conducted to determine an overall risk rating. This will allow organizations to create a prioritized action plan to address those gaps.
- Step 7: Implement the action plan.

The Framework is an iterative process that must be repeated regularly when the impact on the organization or the cyber threat landscape changes. According to the NIST and MITRE, regularly scheduled reviews of the security profile, gap reassessment, updated action plans, and completed action plans should be conducted at least every two years and/or after relevant cybersecurity incidents or discoveries in the industry (Scholl and Suloway, 2022).

6.2. Defining cybersecurity standards for commercial space sector: European approach

At the European level, ENISA (European Union Agency for Cybersecurity) identified space as a sensitive domain in 2023 and acknowledged the fact that the lack of security requirements in the sector has led to a dearth of analysis and control of space-based infrastructure, which poses a significant security threat (ENISA, 2022). ENISA also recognized that without a broader EU-wide focus, building a strong and secure space infrastructure may take too long, leaving space-based vulnerabilities undiscovered and open to exploitation by private companies, governments, or criminal groups. Moreover, ENISA highlighted that those ground stations, which connect satellites to a central terrestrial hub, are a key element that attackers may target with denial-of-service attacks to disrupt critical military and civilian systems. Introducing space-based weapons may further shift the geopolitical paradigm, underscoring the

importance of addressing space-based infrastructure's lack of analysis and control. Attackers may remain dormant until they execute their exploits during a conflict as a means of hybrid warfare.

Despite these warnings, as of the time of writing this paper, there is a notable absence of a comprehensive cybersecurity guideline in the EU that establishes clear technical requirements for commercial space actors. Space-based services have only recently been included in the critical infrastructure taxonomy thanks to the NIS2 Directive (EUDirective, 2022). Given the lack of coordination, many Member States are acting autonomously, providing more or less general guidelines to commercial space companies to address the issue. In Germany, in 2021, the Federal Office for Information Security (BSI) initiated a working group consisting of experts from BSI, OHB Digital Connect, Airbus Defence and Space, and the German Space Agency at the German Aerospace Center (DLR) to jointly develop minimum cybersecurity requirements for satellites (BSI, 2022).

These workshops resulted in the industry-specific IT baseline protection profile in the first step. However, the document provides only general recommendations and is focused on the in-orbit part of the space infrastructure; to address the very different protection needs of various satellite missions and the other segments, it is planned to detail the requirements in various technical guidelines after the creation of the baseline protection profile and to establish them in the international context.

A recent development is represented by the Network and Information Security 2 (NIS2) (EUDirective, 2022) directive, approved in November 2022, by the European Parliament that replaces the previous NIS1. In addition to raising the level of cybersecurity for the entities involved in data security, the new directive recognizes space as critical infrastructure and establishes incident reporting activities to document anomalies found in systems appropriately. The NIS2 Directive recognizes the space sector as an essential entity subject to the EU's most strict cybersecurity requirements. The Directive will have several implications for the sector, as space organizations must comply with new reporting requirements and report any cyber-incidents that could impact the space infrastructure, including satellites and ground stations. This will create new challenges for space organizations regarding monitoring, detecting, and responding to potential cyber threats. The Directive requires greater collaboration and intelligence sharing between the space industry and regulatory bodies to identify and address potential cybersecurity risks and improve the sector's overall cybersecurity and resilience. Given the complex and global nature of the space sector's supply chains, the NIS2 directive also imposes prioritizing supply chain security: Space organizations should implement robust supply chain risk management practices, including monitoring suppliers and third-party contractors. Considering these new obligations, which will be mandatory one year from now, compliance with the NIS2 Directive may create new entry barriers in the space market: Smaller and newer space organizations may find it more challenging to comply with them, potentially leading to market consolidation and changes in the competitive landscape. This could also result in the emergence of new space industry leaders who prioritize cybersecurity and resilience.

Another new feature introduced by the NIS2 will be the possibility of implementing a European cybersecurity certification scheme. According to Article 24, Member States have the authority to mandate that essential or important entities utilize ICT products, services, and processes that meet specific European cybersecurity certification schemes. The European Commission may adopt acts determining the categories of these essential or important entities that must use certified ICT products, services, and processes, or acquire a certificate under a particular European cybersecurity certification scheme. Additionally, the Commission can request ENISA to develop a new certification scheme or review an existing one in situations where no suitable European cybersecurity certification scheme is available. According to the European Telecommunications Standards Institute (ETSI), implementing the Open Security Controls Assessment Language (OSCAL) may be necessary to implement multiple provisions of NIS2 effectively (ETSI, 2023). This is especially relevant for affected essential and important entities that must satisfy various, constantly evolving requirements across diverse contexts (ETSI, 2023). OSCAL is a standardized data-centric framework developed by NIST that can be used to assess the security controls application of an information system. The goal of OSCAL is to overcome the data conversion and manual efforts to describe security control's application and implementation, moving to a machine-readable format, and automating the security assessment process in several scenarios (Piez, 2019).

A significant step has been carried out by the EU at the end of 2022, with the Cyber Resilience Act (European Commission, 2022), a proposed legislation aimed at establishing common standards for connected devices and services not currently covered by regulations such as the NIS2. If approved, the act would impose fines of up to € 15 million (16 million $) or 2.5% of worldwide turnover on non-compliant products. The act classifies products into "default," "Class I," and "Class II" categories.

"Class I" products, such as browsers, password managers, and routers, pose, according to the proposal, minimal security risks. Manufacturers must adhere to specific standards or undergo third-party certification. "Class II" products, including software operating systems, industrial routers, and smart meters, present the highest security risk. They require third-party certification before entering the market. Approximately 90% of digital products fall into this category, even those that do not pose significant cyber threats, like photo editing software and video games. The legislation will be implemented in two phases. Within 12 months of adoption, manufacturers must report cybersecurity breaches and vulnerabilities. Within 24 months, member states and affected businesses must comply with the regulations. Some business groups and member states have raised concerns about the act. They argue that third-party judgment of security measures introduces inherent risks in the certification process. Moreover, critics fear potential delays or hindrances to the rollout of essential new technologies and services, as businesses would need to wait for certification before adopting product security measures (Chiara, 2022).

As much as concerns Network Router Security Threat Analysis, ETSI defined in May 2022 a Threat Vulnerability and Risk Analysis (TVRA) (ETSI, 2023) assessment guidance that can be considered the latest European attempt to define a clear and standardized risk assessment procedure for this type of technology. However, the technical report only discusses the security of network routers that are enterprise routers or ISP routers; the home and small office routers, which forward IP packets between the home computers and the Internet, are out of the scope of the document. The approach to network router risk analysis used by ETSI involves identifying the key assets of network routers and analyzing their vulnerabilities in detail. The key assets of routers are determined by their architecture and main functions. The analysis begins by identifying the threats in different scenarios that include access-side attacks, inter-device horizontal attacks, O&M attacks, supply-chain attacks, and physical attacks. The ETSI document provides guidelines for a detailed risk assessment for a specific network, allowing the network operator to assess the threat level based on the capability and motivation of an attacker to attack these assets. The risk analysis also considers the security challenges faced by network routers, such as the protection of hardware, software, data, and protocols. It examines the vulnerabilities in these areas and provides insights into mitigating the risks associated with them. The TVRA could be considered a useful starting point to build an efficient risk management strategy for SatCom user segment.

6.3. A comparison of the American and European approaches to space cybersecurity

The first point to be discussed when analyzing the two approaches is the lack of a European set of rules and laws for space infrastructure

cybersecurity at the time of writing. In the US, The Satellite Cybersecurity Act (Satellite Cybersecurity Act, 2023), reported to the Senate on June 21st, 2022, addresses cybersecurity concerns about commercial satellite systems. The bill mandates that the Cybersecurity and Infrastructure Security Agency (CISA) creates and maintains a publicly available repository of resources that focuses on the cybersecurity of commercial satellite systems. Additionally, CISA must compile voluntary recommendations for developing, maintaining, and operating these systems, which must include measures for safeguarding against cyber-related vulnerabilities, risks, and attacks. CISA must also implement its activities in collaboration with the private sector wherever possible. The bill further necessitates the Government Accountability Office (GAO) to investigate and release a report on two issues. Firstly, the federal measures taken to support the cybersecurity of commercial satellite systems, particularly in the critical infrastructure sectors, must be studied and reported. Secondly, the government's dependence on commercial satellite systems owned or controlled by foreign entities must be examined. The GAO must coordinate with designated federal agencies to conduct this study and report. In Europe, the only primary source of law dealing with space cybersecurity is the NIS2 Directive. However, how it will be applied and its consequences will be clear only at the end of 2024. Agencies such as ENISA and EUSPA have not yet clearly defined their role and contributions as much as concern SatCom or in general space cybersecurity. Even if Member States are developing their cyber strategies and laws in the field, before developing pan-European space infrastructure, it should be determined a pan-European cyber strategy for space. Considering space as a critical infrastructure pivotal to national security interests, US agencies such as NSA, FBI, and CISA constantly produce advisories, technical reports, and recommendations about SatCom and space cybersecurity, updating users and companies on threats and suspicious activities observed in the wild. At the time of writing, the same activity cannot be observed at the European level, there is no equivalent of a National Security Agency in the EU, where ENISA or EDA could maybe cover such a role.

As much as concern standards in the United States, the NIST produced several resources guiding the sector as the Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NIST IR 8323 (Bartock et al., 2021)), Introduction to Cybersecurity for Commercial Satellite Operations (NIST IR 8270 (Scholl and Suloway, 2022)), and Satellite Ground Segment: Applying the Cybersecurity Framework (CSF) to Assure Satellite Command and Control (NIST IR 8401 (Lightman et al., 2022)).

In Europe, the TVRA produced by ETSI should be adapted to recent threats and scenarios, including satellite modems and routers. For this research, however, it should be considered that approaches vary according to projects and infrastructures, and *IRIS*^{2} will probably be one of the first examples of Member States developing a common set of rules in the sector.

6.4. A wider look: the cybersecurity guidelines for commercial space systems in Japan

The landscape of cybersecurity space policies is constantly evolving, and new standards, recommendations, and guidelines are constantly being developed by States and international organizations. To give the research a wider perspective, we analyze in this section the Cybersecurity Guidelines for Commercial Space Systems developed by the Japanese Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade, and Industry (METI) (Space Industry Office, 2019).

The Guidelines developed by METI depict a complex scenario where more than 90 security incidents occurred both inside and outside Japan between 1986 and 2022 with a significant increase in the last 5 years. According to the Japanese authorities, the critical and challenging nature of cybersecurity for space systems is underscored by several main factors. These include the expanding roles of space systems in Japan's security, economy, and society, the proliferation of digital technology such as unmanned and automated space systems along with increased cloud services usage, the growing complexity of networks including inter-satellite communication and connections with ground communication networks, the rise in the number of satellites, ground stations, and data volume due to satellite constellations, and the increased complexity of supply chains resulting from the commercialization of space systems technology and the incorporation of consumer technology.

The purpose of these Guidelines is to collect essential information in an accessible format. Key elements covered by these guidelines encompass examining and presenting security risks associated with space systems. Furthermore, the guidelines delineate fundamental security measures that should be scrutinized by all stakeholders involved in the intricate web of space systems.

The guidelines cover satellite systems and ground systems, including satellite operation facilities, satellite data utilization facilities, and development and manufacturing facilities operated by the commercial sector. They apply to the entire lifecycle of satellite systems, including design, development, manufacturing, operation, maintenance, and disposal phases. It is important to note that the launch facility is not covered in the document.

A relevant difference between the previously analyzed approaches is that METI uses the Cyber/Physical Security Framework (CPSF) Ver. 1.0 (Cyber Security Division, 2019) to address cybersecurity risks in commercial space systems. This is a multi-stakeholder approach that ensures the security of the entire supply chain, including affiliated companies and business partners. CPSF considers the industrial society in three layers and organizes risk sources and measures at each layer. The layers are structured as follows:

- First Layer: Connections between organizations
- Second Layer: Mutual connections between Cyberspace and Physical space
- Third Layer: Connections in Cyberspace

In the first part of the Guidelines, seven example risk scenarios are included, and for each of them, a series of measures for each of the three layers is defined. The document also defines a series of Cybersecurity requirements and basic measures connected to it to be implemented. This technical approach links each measure/requirement with the stakeholders that should be involved in it. An interesting tool proposed by METI is the Cybersecurity Management Guidelines Implementation Status Visualization Tool, a table that can be used to assess the company's efforts on 10 key items. This tool is for enterprises and organizations with 300+ employees. It has 40 questions and uses a 5-point scale to measure the status of measures taken. The Japanese approach to cybersecurity for space systems and networks is highly technical and practical. However, the complexity of the process can be a challenge for companies that need to navigate through it. To overcome this, companies may need to develop automated checking and verification tools based on the Guidelines. This approach is one of the first attempts by a sovereign nation to develop clear guidelines for the sector. It provides non-trivial examples of threat scenarios that can affect space infrastructure and systems. It is important to note that Japan like the rest of the countries analyzed does not have any legally binding cybersecurity requirements for space companies. The guidelines provided in the document are optional, meaning that companies are free to follow them or not. However, even if they choose to follow international standards, it may not be enough to ensure the safety of space infrastructure, as we have seen in the past. The current state of space cybersecurity policies is constantly changing. In Europe, most countries and space agencies are still developing their cybersecurity toolkits. While the Union may establish a Space Law, it may be beneficial to examine the approaches taken by other countries, such as Japan, and push member states to work together to prevent any harmonization-related problems in the future. As the policy and in-

dustrial landscape continue to evolve future research should be carried out to compare the new standards, technical guidelines and policies in the field, having also a wider look and including the activities of non western countries to understand their priorities and threat perception.

7. Lessons learned to build a resilient European satellite communication constellation

Cyber risk management for space systems is complex and challenging, as ground stations and user terminals are exposed to a wide range of cyber threats and vulnerabilities. When developing *IRIS*^{2}, the new space infrastructure for secure communication, the EU should consider some of the key challenges associated with cyber risk management. As the main point, the complexity of the space ecosystem should never be underestimated as it involves a large number of stakeholders, including governments, private companies, and international organizations. This complexity makes it difficult to implement a unified approach to cyber risk management, as different stakeholders may have different priorities and resources. This is extremely relevant for *IRIS*^{2} since this constellation will be implemented through the support of the private sector probably with commercial solutions already available on the market. Moreover, the space sector is subject to a rapidly evolving threat landscape, with new threats and vulnerabilities emerging regularly. Keeping up with them is challenging, particularly for organizations with limited resources. As already mentioned, a weak spot is represented by supply chain vulnerabilities as ground and user segments rely on a complex supply chain. Malicious actors may target the supply chain to gain access to the ground station, compromise the hardware or software, or steal sensitive data. In this, as in any other scenario, human error and insider threats can pose a significant risk. Staff members may accidentally introduce vulnerabilities or may be targeted by malicious actors seeking to gain unauthorized access to the system. To manage cyber risks effectively, all the actors involved in the management, administration, and functioning of space infrastructure should implement a range of best practices that we report briefly below.

7.1. Access control

A first best practice consists of implementing access controls to limit access to critical systems and data to authorized personnel only. Access controls should be based on the *principle of least privilege*, meaning that staff members are only given access to the systems and data they need to perform their job duties. Since network perimeter devices are crucial components in securing a network, Access Control Lists (ACLs) should be configured to make them work together and regulate inbound and outbound traffic. These access control rule sets should be specifically configured to allow only necessary services and systems to support the network's mission. It should be recommended to use a deny-by-default, permit-by-exception approach, which involves carefully selecting which connections to allow and then creating rule sets that focus on allowing only those connections. This approach allows a single rule to deny multiple types of connections, reducing the need to create separate rules for each blocked connection. Failure to adopt this approach can lead to unnecessary access, increasing the risk of compromise and information gathering. If additional perimeter rule sets are needed dynamically, an intrusion prevention system (IPS) should be put in place to prevent adversaries from exploiting the network. It is also recommended to enable logging on all rule sets that deny or drop network traffic, as well as on successful and unsuccessful administrator access to critical devices. A network access control (NAC) solution should be implemented to prevent unauthorized access to a network. Such a solution prevents unauthorized physical connections and monitors authorized physical connections in the network. Port security can be implemented on switches to detect unauthorized devices connected to the network via a device's media access control (MAC) address.

7.2. Network segmentation

Segmenting the network is needed to ensure that critical systems and data are isolated from non-critical ones. This can limit the impact of a cyber attack, as the attacker will only have access to a limited portion of the network. Moreover, critical systems should be physically separated from other networks like the Internet. Internal routers, switches, and firewalls should be restricted to only allow necessary ports and protocols for valid mission needs. To protect against lateral movement by attackers within a network, similar systems should be grouped together logically. Network segmentation reduces the likelihood of such attacks, as it limits the ability of attackers to exploit other systems. The CISA and the NSA recommend logical grouping through isolation of similar systems into different subnets or VLANs, or physical separation using firewalls or filtering routers. This approach makes access restrictions between systems easier to manage, control, and monitor. Access control lists can be duplicated and applied directly to switches to limit access between VLANs, or they can be applied to core routers for routing between internal subnets.

7.3. Encryption

Encrypting sensitive data both at rest and in transit prevent unauthorized access and ensure confidentiality and integrity of data. The main guidelines for encryption have been described in the dedicated section above. The Committee on National Security Systems Policy (CNSSP) 15 has established minimum recommended settings for ensuring robust encryption in these networks. According to CNSSP 15, it is necessary to use Diffie-Hellman Group 16 with 4096 bit Modular Exponent (MODP) and Diffie-Hellman Group 20 with 384 bit elliptic curve group (ECP) for secure key exchange. Additionally, Advanced Encryption Standard (AES)-256 should be used for encryption, and Secure Hash Algorithm (SHA)-384 for hashing. At the time of writing, by adhering to these recommendations, SatCom networks can achieve the highest levels of security and protection against unauthorized access and data breaches.

7.4. Continuous monitoring

Implementing continuous monitoring to detect and respond to cyber incidents can involve the use of intrusion detection systems, security information, and event management (SIEM) systems, and threat intelligence feeds. Operators should not only monitor their network but stay updated on recent CVEs and exploit published as well as password leaks. These last steps may be implemented by monitoring notorious blogs and forums on the dark web, where these data are often published.

7.5. Incident response

Developing an incident response plan to ensure that cyber incidents are detected and responded to in a timely and effective manner. The incident response plan should cover areas such as incident notification, escalation, investigation, and communication. The prompt detection and response of an incident are pivotal in determining the impact of an attack. In the event of detecting a breach before the deployment of wiper malware, the effectiveness of the incident response team's handling and response to the alert can make all the difference between preventing data loss and facing complete data destruction.

7.6. Regular patching and updating

Regularly patching and updating user segment modems, and routers with the latest security updates and firmware will help to ensure that the network is protected against the latest security threats and vulnerabilities. Software must be designed to be patch friendly and provide confidence for operators to patch frequently and safely.

7.7. Training and awareness programs

Staff training and awareness programs are essential to ensure that employees are aware of the latest cybersecurity threats and how to identify and report potential cyber incidents. The policy should cover regular training sessions, simulated phishing exercises, and best practices for secure data handling.

7.8. Establishing a well-defined cybersecurity policy

Developing clear policies, procedures, and guidelines for managing cyber risks is critical for any organization. Cybersecurity policies and procedures define the rules and expectations that employees and third-party contractors must follow to maintain the security of ground station systems and data. A comprehensive cybersecurity policy should cover several aspects, including access controls, incident response, data classification, and training and awareness programs. In this context, policies should not be aimed at regulating any aspect of space systems, including technical details, but specifying what standards and requirements operators should choose when developing space infrastructure.

7.9. How public sector support can help implement crucial measures

Often the implementation of the basic security practices in the commercial SatCom industry has been overlooked, primarily due to a variety of possible reasons. The complexity of SatCom systems, involving cutting-edge technology and large-scale distributed networks, poses a significant challenge in implementing security measures. Budgetary constraints also play a role, as the cost of implementing extensive cybersecurity measures can be prohibitive for some organizations, leading them to underfund cybersecurity initiatives. In swiftly moving sectors, businesses may choose to prioritize speed-to-market over implementing strict security controls, thereby leaving security gaps. Lastly, in some instances, the regulatory environment in the satellite communications industry might not have kept pace with the rapidly evolving threats, causing an absence of mandatory security practices. These potential reasons, among others, underscore the urgent necessity for a thorough analysis of cybersecurity practices in the SatCom industry.

As analyzed, security controls and standards in the field are starting to be developed. However, just because they exist, it does not mean they are implemented and enforced. Considering the complexity of space infrastructures and their interconnectedness with other critical domains, what emerges are the challenges arising for companies to perform extensive and effective cybersecurity risk assessments and analyses without external partners (Kapalidis et al., 2019). This should not be intended only as consultancy services and outsourcing but as the need to implement strong relationship and cooperation mechanisms with institutions and governmental agencies.

With this in mind, the Viasat case underscored several crucial lessons and managerial implications for companies. First of all, it showed how well public-private partnerships can work in responding to cyber-attacks. Part of Viasat's response plan involved collaborating and exchanging information with various government bodies, intelligence units, and law enforcement agencies. The National Security Agency's Cybersecurity Collaboration Center (NSA CCC) had an established relationship with Viasat (Brumfield, 2023). They promptly engaged after the attack, working alongside the Viasat team to discuss and analyze incoming data and insights. Furthermore, they aided in disseminating this information across different agencies. The NSA independently used the insights and data provided by Viasat, both immediately and in the subsequent months, to conduct its own analysis. This allowed them to identify connections to known threat actors, comprehend cyber threats more comprehensively, and offer additional mitigation guidance to a wider audience. For Viasat, understanding what constitutes "normal" operations proved invaluable in narrowing down their response. This knowledge facilitated the identification of abnormal actions, such as unusual file transfers or atypical toolkit usage, providing critical insight into the attack's nature. However, many companies lack a clear inventory of assets or a comprehensive grasp of their normal operations, hindering swift response strategies (Olivero, 2022). Automated tools for these tasks exist but have not been widely applied in the space sector (Coulter et al., 2019; Waedt et al., 2016).

Taking these lessons into account, what may be lacking in Europe is a strong and established dialogue between companies and institutions, but also among companies themselves. Suppose we consider budget constraints as being one of the main barriers to standards and control implementation. In that case, these obstacles can be reduced significantly by implementing cooperative solutions or peer learning strategies.

European policymakers realized the importance of cooperation mechanisms: in October 2023 the Commission and EUSPA established the EU Space Information Sharing Centre (ISAC) (EUSPA , 2023), a collaborative initiative aimed at fostering information exchange, promoting collaboration, and advocating best practices among private organizations. Its core objectives include sharing insights on security, cyber incidents, and vulnerabilities, offering early warning systems, and enhancing cybersecurity resilience through shared knowledge and expertise. Participation is open to founding members (legal private entities from the Space sector established in the EU), academic institutions, and recognized bodies with space security expertise. Public partners, including institutions, agencies, and national Space Agencies, are also welcome to collaborate in solving cybersecurity challenges. Such initiatives can significantly reduce the financial burden of small and medium-sized space companies, facilitating information exchange and even peer learning in the sector. However, the limits of such an initiative are clear; even if the EU ISAC will propose ready-to-use and actionable resources and tools for participants, including to guide the implementation of relevant EU regulations and shared best practices, it will not be an incident response body. Providing an answer to a security incident will remain the responsibility of each Member/company.

The Satellite Cybersecurity Act mentioned in Section 6.3 can be considered as a similar initiative in the US, with the sole difference that the American approach envisioned a stable office and staff to develop its tasks. An idea of the financial implications of the initiative is given by the Congressional Budget Office's (CBO) analysis (Congressional Budget Office, 2023), which foresees 6 full-time employees to develop and oversee the online database housing cybersecurity resources for satellite operators described in the Act. The anticipated annual costs for staff salaries and technology needed to publish safety materials are estimated at $3 million. The CBO approximates an expenditure of $14 million from 2023 to 2028 for implementing the bill. ENISA or EUSPA in Europe have not conducted similar estimates, and there are no indicators to suggest a similar investment in support of the European sector. This significantly limits the capabilities of the Space ISAC in comparison.

7.10. Navigating regulatory challenges: how companies are adapting to the evolving landscape

Lawmakers across Europe and the rest of the World have started drafting space laws that incorporate basic or advanced cybersecurity requirements for the sector. However, at the time of writing, the Space Law in Europe is still in its early stages. The European Commission has asked the industry to share its views on four different options (European Commission, 2023), two of which involve the creation of binding rules and detailed technical standards developed by the European Standardisation Organisations. The proposed options would require satellite operators, manufacturers, and Member States Authorities to comply with mandatory cybersecurity regulations. The implementation of this act may have negative managerial implications that could hinder the sector's steady growth, which is expected to continue in the future. A clear assessment of the impact of this Law on the sector has not been de-

veloped, but a possible comparison with similar regulations is possible using ENISA's study on the effects of the NIS (ENISA, 2023). ENISA measured that the NIS had a positive impact on cybersecurity investments for many sectors. In particular, in 2023 Operators of Essential Services (OES) and Digital Service Providers (DSP) earmark 7,1% of their IT investments for Information Security, an increase of 0.4% compared to last 2022 (ENISA, 2023). Similar studies highlighted how the effect of NIS2 may require a 0,92% turnover as compliance cost (Frontiers Economics, 2023), a similar increase if provoked by the future Space Law, may impact negatively the SMEs in the space sectors.

The Industry, especially the New Space sector expressed caution toward the future Space Law, encouraging the application of different cybersecurity standards tailored to each space mission's unique needs, as less stringent standards for commercial missions in LEO, and more high-security ones for those in GEO (Y.E.E.S. Space, 2023). However, such an approach may be challenged by the dual use of constellations such as the Viasat one or by their multi-orbital nature as in the case of $IRIS^2$. Overall the sector seems to approve a cybersecurity-by-design process in program management, and in mission operations, but recommends introducing mission-tailored higher cybersecurity labels without applying them to the entire industry (Y.E.E.S. Space, 2023). Without any doubt, adhering to certain aspects of the law will cause an increase in the costs of data, satellites, and services for companies involved in the whole space value chain. There are uncertainties as to whether any measures will be undertaken by the institutions to alleviate the costs associated with compliance, to ensure that European companies do not face any disadvantage in the global market (EARSC, 2023).

Taking a closer look at the attitude of companies towards these new challenges, it is clear how many of them are changing their risk appetite towards cybersecurity risks due to increased attacks. Looking at the financial reports of industry leaders such as Viasat (Viasat, 2023) or Eutelesat (Eutelsat, 2023), cybersecurity is now part of their risk factors lists. Companies realized that cybersecurity *"requires significant management attention and resources to remedy the damage that results and delay progress on business objectives and may cause companies to make payments to their customers to reimburse them for damages, pay them penalties or provide refunds; and provoke damage to their reputation with their customers (particularly agencies of the U.S. government) and the public generally"* (Comtech, 2023b).

To mitigate these risks, companies started hiring professionals such as Chief Information Security Officers, Cyber Accreditation Officers, Cyber Risk and Security Engineers, Security Operations Managers, or even engineers to comply with specific US procurement processes (Eutelsat, 2023). Space companies are also increasing the involvement of researchers and cybersecurity professionals. In the US the Department of Defense recently sponsored a competition for white hat hackers to attempt to breach an active satellite (Gedeon, 2023). While industry leaders are opening bug bounty programs to speed up the discovery of vulnerabilities in their systems (Starlink, 2023). However, small and medium-sized companies in Europe may not have the resources to implement these actions.

Based on our analysis, we can conclude that the security aspect of space is facing a significant issue of fragmentation. This problem mainly concerns the stakeholders and governance of the sector, which could potentially hinder the public-private partnership essential for its growth. The European Union and national governments are finding it challenging to regulate and control the dissemination of technology in space and other sectors. The number of states with space programs has grown significantly, from the original 2 to approximately 70 in 2022 (Eriksson and Giacomello, 2022), and the rise of private corporations and non-governmental organizations in space has contributed to a more scattered group of stakeholders. Governance can be quite fragmented, especially in Europe and in the cyber domain. We can observe this by looking at the separation of cyberspace and space, as well as the confused interaction and role definitions among the Commission, ENISA, and EUSPA. This fragmentation can create uncertainty, as companies are not certain about the processes they should be involved in, the standards they should implement, or the jurisdiction, harmonization, and costs of new regulations.

The complexity of space systems, high cybersecurity costs, and unclear regulations make it necessary for the public and private sectors to work together more closely. On one side, space companies need to communicate their needs and inform stakeholders about the kind of support they require. On the other hand, EU institutions and agencies need to establish clear governance and tools to not only support the industry but also develop cyber risk strategies with it. Implementing strong regulations and standards can bring about significant changes in the cybersecurity of the space industry. However, as with other sectors, there is a trade-off between security and technological progress. The EU needs to exhibit political commitment and allocate appropriate resources to support the industry without hindering growth or burdening businesses with excessive financial or regulatory demands that they cannot manage.

All in all, determining the root causes behind the lack of security measures implementation in space is not an easy task. However, research has indicated that the space sector cannot achieve a high level of security on its own and requires greater public support. Regulators need to consider the complexity and fragmentation of the sector and not increase them while designing new policies. Preliminary attempts to address security in this domain show that initiatives that involve cooperation between the public and private sectors can help enhance security measures. These initiatives include enhanced information-sharing capacities, implementation of online databases with cybersecurity resources for satellite operators, the establishment of a clear inventory of assets and normal operations, state sponsored ethical hacking competitions, bug bounty programs, enhanced hiring capacity for cybersecurity experts, and the inclusion of cyber risks in the financial considerations of companies. These actions are not to be considered just optional but essential to improve space resilience and prevent disruptions. However, the low maturity level of these initiatives (many of them are still in the early stages and not widely adopted) may partially explain the lack of security in the space sector, together with the appearance of new, more complex, and frequent space threats.

8. Related work

Numerous studies have recently been carried out in the field of SatCom cybersecurity. Tedeschi et al. (2022) provide a comprehensive overview of the link-layer security threats, solutions, and challenges faced when deploying and operating satellite-based communication systems. Their work covers various domains related to satellite cybersecurity, including physical-layer security, cryptography schemes, anti-jamming strategies, anti-spoofing techniques, and quantum-based key distribution schemes. The paper highlights the most essential techniques, peculiarities, advantages, lessons learned, and future directions in each of these domains.

Benitez (2021) addresses the cyber security risks present in VSAT terminals and provides methods for users to secure their data transmission through VSAT networks. The research also includes a literature review of publications about vulnerabilities in VSAT systems by cyber security organizations, VSAT service providers, and satellite communication market research.

Comprehensive and pioneering research on the field is the one by Santamarta (2018) that provides an in-depth analysis of the vulnerabilities and risks associated with SatCom security. He explains how attackers can exploit these vulnerabilities to gain unauthorized access to sensitive information, disrupt communication networks, and compromise safety. The paper also highlights the importance of responsible practices and proactive measures to prevent such attacks. The document focuses on a specific aspect of SatCom security. Furthermore, the paper discusses the impact of SatCom security on aviation, maritime, and military sectors. Although the white paper serves as a valuable resource

Table 5
Literature Source.

Literature Source	Focus on User segment	Considers IRIS^2 and its implications	Provides legislative approach	In-field analysis
Tedeschi et al. (2022)	✓	✗	✗	✗
Benitez (2021)	✓	✗	✗	✗
Santamarta (2018)	✓	✗	✗	✗
Smailes et al. (2023)	✓	✗	✗	✗
Jacobs (2023)	✗	✗	✗	✓
This paper	✓	✓	✓	✓

for anyone interested in understanding the importance of SatCom security and its impact on various industries, the research is focused on a limited number of terminals and is not updated, even if the majority of those terminals are still operational today.

One of the few recent works that focused on modem vulnerabilities in SatCom is by Smailes et al. (2023). Their study focuses on the security vulnerabilities of the Starlink user terminal, a satellite modem used for Internet connectivity. The authors audit the attack surface presented by the Starlink router's admin interface and use fuzzing to uncover a denial-of-service attack. They explored the impact of this attack on different scenarios and provided recommendations to better secure satellite routers. The paper also discusses wider implications and lessons learned in terrestrial router security that can be applied in this new context.

Interesting research has been carried out in different fields such as aviation and maritime security. Dave et al. (2022) discuss the increasing vulnerability of the aviation sector to cyber attacks, particularly in the areas of communication, navigation, and surveillance systems. The authors provide an overview of the aviation system and the wireless technologies used, as well as the associated security issues. They also identify threats, attack taxonomy, and existing security frameworks and solutions in the aviation domain. While the paper does not specifically focus on SatCom cyber security, this area is included in the broader discussion of communication system vulnerabilities. In the maritime domain, Caprolu et al. (2020) developed a comprehensive investigation of cybersecurity issues associated with modern vessel systems. It analyzes the communication technologies and computer systems used within large vessels, pointing out several security issues rooted in their design and operational mode. The paper also relates these vulnerabilities with recent incidents and attacks involving vessels and identifies the weak points that any modern vessel needs to mitigate toward the enforcement of the latest IMO resolutions. The paper deals with SatCom cybersecurity by discussing the vulnerabilities of communication technologies on vessels and the security requirements for SatCom datalink systems for future air traffic management.

Now we compare the present paper with the papers mentioned above and summarize the comparison in Table 5. The current paper's main novelty is that it considers the new European multi-orbital constellation for satellite communication *IRIS*^{2} and the political implications of cyber risk in the field of a European SatCom infrastructure. Modem and router security has seldom been addressed in the field of SatCom, while attacks on these components are revealed to be common. Lastly, the works above still lack an accurate cybersecurity assessment of commercial SatCom networks that may be exposed to threats, this is also due to the NIS2 incident reporting requirements that are still not mandatory for the sector. Moreover, they miss a comparison with a clear set of rules and standards at the European level that can be part of the European strategy for space and defence. In conclusion, the user segment has lately been neglected by researchers as recent works on this part of the infrastructure are missing.

9. Conclusions and future work

In the first part of this paper, we described the composition and use cases of SatCom technologies, and we later focused on the user segment component. We highlighted the need for increased research in the field of cybersecurity for space infrastructures, particularly in the user and ground segments of satellite communication systems. The paper discussed the vulnerabilities and risks associated with these components, highlighting the lack of cyber posture in the sector. It also explored the impact of attacks on different scenarios and provided recommendations for securing satellite routers. The paper closely analyzed the case study of the attack on the Viasat network in Ukraine, collecting important lessons and recommendations for future cybersecurity researchers and policymakers that aim to design policies to protect the European space infrastructures such as *IRIS*^{2}.

The research emphasizes the importance of accurate cybersecurity assessments and the development of clear rules and standards at the European level. Comparing various cybersecurity frameworks and some of the first standards for the sector the paper addressed the urgent need for a dedicated risk assessment strategy that could focus on the last component of the SatCom chain, the user segment. We addressed how, in this setting, the NIS2 Directive's obligations could deal with some but not all of the needs to secure the infrastructure. We highlighted the need for constant supervision and active monitoring that should be conducted by entities such as CISA in the United States.

In conclusion, the analysis of the Viasat case study highlighted the implications of SatCom security in several sectors and the cascading effects that an attack can have on energy, transport, and civil security to cite some. The paper highlighted the vulnerabilities that affect some of the user segment components on the field through the use of search engines such as Shodan, showcasing how a big part of the commercial infrastructure can be easily accessible by attackers. Overall, the paper calls for a comprehensive risk assessment strategy and the implementation of guidelines to enhance the security of commercial SatCom networks in view of the new European projects such as *IRIS*^{2}.

Despite addressing several gaps in the current research, the present work could be further extended, deepening the analysis carried out with Shodan, maybe using other tools or performing penetration testing on some of the assets found.

In addition, it is important for future research to focus on obtaining empirical data and real-world scenarios in the field. This can be done by creating a comprehensive dataset of vulnerabilities, breaches, and cyber incidents affecting the sector. Such a dataset can help map out threats, actors, and trends more accurately.

Moreover, future research could address the lack of a specific cybersecurity framework focused on the ground and user segment. The managerial and theoretical implications that may result from implementing robust cybersecurity practices in the field may also be further investigated.

The comparative legislative analysis should expand to include non-western countries such as India and China, which are emerging as new space powers (Stroikos, 2023).

Finally, future work may explore the implications of AI in the field, supporting companies and facilitating the implementation and enforcement of new laws and standards. AI escalating capabilities carry the promise to bolster cybersecurity through enhanced threat detection, automated response systems, and enriched strategic protocols and procedures (Carlo et al., 2023).

CRediT authorship contribution statement

Francesco Casaril: Writing – review & editing, Methodology, Investigation, Formal analysis, Conceptualization. **Letterio Galletta:** Writing – review & editing, Conceptualization.

Declaration of competing interest

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

Data availability

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

Acknowledgements

We thank the anonymous reviewers for their careful and helpful comments and suggestions. This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

Air and Space Forces, 2023. Backdoor to attack satellites: CSO highlights ground networks. https://www.airandspaceforces.com/backdoor-to-attack-satellites-cso-highlights-ground-networks/. (Accessed July 2023).

Akre, Sejal, 2022. Satellite communication market information by product, technology, end-use, and region-forecast to 2025. https://www.marketresearchfuture.com/reports/satellite-communication-market-8466. (Accessed July 2023).

Apache Software Foundation, 2023. CVE-2023-25690, National Vulnerability Database (NVD). https://nvd.nist.gov/vuln/detail/CVE-2023-25690.

Bartock, M., Lightman, S., Li-Baboud, Y.-S., McCarthy, J., Reczek, K., Brule, J., Northrip, D., Scholz, A., Suloway, T., 2021. Foundational PNT profile: applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services, NISTIR NISTIR 8323, national institute of standards and technology (NIST). https://doi.org/10.6028/NIST.IR.8323. superseded by: NISTIR 8323 Rev. 1(01/31/2023).

Benaroch, M., 2020. Cybersecurity risk in it outsourcing—challenges and emerging realities. In: Information Systems Outsourcing: The Era of Digital Transformation, pp. 313–334.

Benitez, R.C., 2021. Cyber Vulnerabilities in Satellite Communication Networks. Master's thesis. Utica College.

Bennett, M., Van Den Hoek, J., Zhao, B., Prishchepov, A., 2022. Improving satellite monitoring of armed conflicts. Earth's Future 10, e2022EF002904.

BleepingComputer, 2021. Hackers leak passwords for 500,000 fortinet VPN accounts. https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/. (Accessed July 2023).

Boschetti, N., Gordon, N.G., Falco, G., 2022. Space cybersecurity lessons learned from the viasat cyberattack. In: ASCEND 2022, p. 4380.

Broad Band Forum, 2020. TR-069 CPE WAN Management Protocol, https://www.broadband-forum.org/download/TR-069_Amendment-2.pdf. (Accessed July 2023).

Brumfield, Cynthia, 2023. Incident response lessons learned from the Russian attack on viasat. https://www.csoonline.com/article/649714/incident-response-lessons-learned-from-the-russian-attack-on-viasat.html. (Accessed 10 December 2023).

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022. IT-Grundschutz-Profil für Weltrauminfrastrukturen. Technical Report, Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html.

C. on National Security Systems, 2016. CNSSP 15, national security systems, use of public standards for secure information sharing, technical report, committee on national security systems. https://nsarchive.gwu.edu/sites/default/files/documents/3521685/Document-08-Committee-on-National-Security.pdf.

Calcutt, D., Tetley, L., 1994. Satellite Communications: Principles and Applications. Butterworth-Heinemann.

Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., Tedeschi, P., 2020. Vessels cybersecurity: issues, challenges, and the road ahead. IEEE Commun. Mag. 58, 90–96.

Carlo, A., Mantı, N.P., Wam, B.A.S., Casamassima, F., Boschetti, N., Breda, P., Rahloff, T., 2023. The importance of cybersecurity frameworks to regulate emergent ai technologies for space applications. J. Space Saf. Eng.

CFR13636, 2013. Cfr 13636 - executive order 13636 of February 12, 2013. Improving critical infrastructure cybersecurity. Fed. Regist. 78 (33).

Chiara, P.G., 2022. The cyber resilience act: the eu commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: an introduction. Int. Cybersecurity Law Rev. 3, 255–272.

Chini, P., Giambene, G., Kota, S., 2010. A survey on mobile satellite systems. Int. J. Satell. Commun. Netw. 28, 29–57.

Common Vulnerabilities and Exposures (CVE), 2018. CVE-2018-13379. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379. (Accessed July 2023).

Comsys, 2010. 12th edition. The comsys vsat report, vsat statistics. https://www.comsys.co.uk/wvr_stat.htm. (Accessed July 2023).

Comtech, 2023a. Comtech ef data - satellite modems. https://www.comtechefdata.com/products/satellite-modems. (Accessed July 2023).

Comtech, 2023b. 10-q quarterly report - 2024 q1, access the quarterly report via the U.S. Securities and exchange commission (SEC). https://s3.amazonaws.com/sec.irpass.cc/2718/0000023197-23-000070.htm.

Council of the European Union, 2022. A strategic compass for security and defence, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

Congressional Budget Office, 2023. Congressional budget office cost estimate. https://www.cbo.gov/publication/59203. (Accessed July 2023).

ConnexionFrance, 2022. Thousands in France lose Internet in suspected Russian cyberattack. https://www.connexionfrance.com/article/French-news/Thousands-in-France-lose-internet-in-suspected-Russian-cyberattack. (Accessed July 2023).

Cooper, D.A., Apon, D.C., Dang, Q.H., Davidson, M.S., Dworkin, M.J., Miller, C.A., 2020. NIST Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes. NIST Special Publication 800-208 Computer Security Division, Information Technology Laboratory. https://doi.org/10.6028/NIST.SP.800-208.

Corcoran, L., Jenkins, M., 2022. Rfc 9206 commercial national security algorithm (cnsa) suite cryptography for Internet protocol security (ipsec). https://datatracker.ietf.org/doc/rfc9206/. (Accessed July 2023).

Correia, R., Varum, T., Matos, J.N., Oliveira, A., Carvalho, N.B., 2022. User terminal segments for low-Earth orbit satellite constellations: commercial systems and innovative research ideas. IEEE Microw. Mag. 23, 47–58.

Coulter, R., Han, Q.-L., Pan, L., Zhang, J., Xiang, Y., 2019. Data-driven cyber security in perspective-intelligent traffic analysis. IEEE Trans. Cybern. 50, 3081–3093.

Criscuolo, E., Hogie, K., Parise, R., 2001. Transport Protocols and Applications for Internet Use in Space. 2001 IEEE Aerospace Conference Proceedings, vol. 2. IEEE, pp. 2–951 (Cat. No. 01TH8542).

Cyber Security Division, 2019. Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, the cyber/physical security framework.

Dacey, R.F., 2002. Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed. Diane Publishing.

Dave, G., Choudhary, G., Sihag, V., You, I., Choo, K.-K.R., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. Comput. Secur. 112, 102516.

Debruin, J., 2008. Control systems for mobile satcom antennas. IEEE Control Syst. Mag. 28, 86–101.

Donner, A., Berioli, M., Werner, M., 2004. MPLS-based satellite constellation networks. IEEE J. Sel. Areas Commun. 22, 438–448.

EARSC, 2023. Earsc position on the eu space law – new rules for safe, resilient, and sustainable space activities. https://earsc-portal.eu/display/EOwiki/Policy+Observatory?preview=/131531853/173342985/090166e5041a1b9d.pdf. (Accessed 14 December 2023).

ENERCON, 2022. Over 95following disruption to satellite communication. https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/. (Accessed July 2023).

European Union Agency for Cybersecurity (ENISA), 2022. ENISA Threat Landscape 2022, Technical Report, ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Eriksson, J., Giacomello, G., 2022. Cyberspace in space: fragmentation, vulnerability, and uncertainty. In: Cyber Security Politics. Routledge, pp. 95–108.

Eshwari, A.P., Shrivastava, A., 2017. Application of satellite communication & remote sensing for development. J. Pure Appl. Ind. Phys. 7, 224–238.

ETSI, 2024. Satellite Earth Stations and Systems (SES), Broadband Satellite Multimedia (BSM) services and architectures Functional architecture for IP internetworking with BSM networks Technical Report TS 102 292, European Telecommunications Standards Institute (ETSI), p. 292.

EUDirective 2022:2555, 2022. Directive (eu) 2022/2555 of the European Parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the union, EUR-lex. https://eur-lex.europa.eu/eli/dir/2022/2555. (Accessed July 2023).

European Commission, 2022. Proposal for a regulation of the European Parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020. COM(2022) 454 final. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf. (Accessed July 2023).

European Commission, 2023. Targeted consultation on eu space law. https://defence-industry-space.ec.europa.eu/consultations-0/targeted-consultation-eu-space-law.

European Parliament and Council, 2022. Directive (eu) 2022/2557 of the European Parliament and of the council of 14 December 2022 on the resilience of critical entities and repealing council directive 2008/114/ec. Off. J. Eur. Union. http://data.europa.eu/eli/dir/2022/2557/oj.

European Telecommunications Standards Institute (ETSI), 2023. ETSI TR 103 866 V1.1.1 (2023-02), cyber security (CYBER); implementation of the revised network and information security (NIS2) directive applying critical security controls. Technical Report 103 866 V1.1.1, European Telecommunications Standards Institute (ETSI), Available at https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf.

European Union, 2021. Regulation (eu) 2021/696 establishing the eu space programme and the European Union agency for the space programme. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.157.01.0001.01.ENG. (Accessed July 2023).

European Union Agency for Cybersecurity (ENISA), 2023. Nis investments report. https://www.enisa.Europa.eu/publications/nis-investments-2023.

EUSPA, 2023. Call for expressions of interest: Eu space information sharing and analysis centre (eu space isac). https://www.euspa.europa.eu/opportunities/isac. (Accessed 19 September 2023). Version: 1.5.

Eutelsat, 2023. Reference document - universal registration document, access the document via Eutelsat. https://www.eutelsat.com/files/EUTELSAT_BAT%2020-10_UK.pdf.

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

FBI-CISA, 2021. APT actors exploit vulnerabilities to gain initial access for future attacks. https://www.ic3.gov/Media/News/2021/210402.pdf. (Accessed July 2023).

Fernández-Caramés, T.M., Fraga-Lamas, P., 2020. Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. Sensors 20, 3048.

Finch, P.E., Sullivan, D.V., Ivancic, W.D., 2012. An evaluation of protocol enhancing proxies and modern file transport protocols for geostationary satellite communication. In: 2012 IEEE Aerospace Conference. IEEE, pp. 1–8.

Fortinet, 2023. Malicious Actor Discloses FortiGate SSL-VPN Credentials, 2021. https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials. (Accessed July 2023).

Fritz, J., 2013. Satellite hacking: a guide for the perplexed. Cult. Mandala 10, 5906.

Frontiers Economics, 2023. Assessing the economic impact of eu initiatives on cybersecurity. https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf. (Accessed 10 December 2023).

Gedeon, J., 2023. For the first time, U.S. government lets hackers break into satellite in space. https://www.politico.com/news/2023/08/11/def-con-hackers-space-force-00110919. (Accessed 10 December 2023).

Giray, S.M., 2013. Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In: 2013 6th International Conference on Recent Advances in Space Technologies (RAST). IEEE, pp. 795–800.

Gopal, R., Ravishankar, C., Huang, X., 2022. Smart Network Connectivity for Hybrid Space and Terrestrial Connectivity. In: 39th International Communications Satellite Systems Conference (ICSSC 2022). IET, pp. 84–90.

Heissler, J., Marshall, J., Piccola, R.M., Sonalkar, R.V., Zeng, J., 2005. A performance analysis on the application of commercial standards for ip satcom modems. In: MILCOM 2005-2005 IEEE Military Communications Conference. IEEE, pp. 787–793.

Hughes, 2023. Hughes - mobile satellite terminals. https://www.hughes.com/what-we-offer/satellite-ground-systems/mobile-satellite-terminals. (Accessed July 2023).

Hurova, A., 2022. Earth observation for the protection of human rights during the armed aggression. Adv. Space Law 9.

I.O. for Standardization, I.E. Commission, 2022. Iso/iec 27002:2022 information technology— security techniques—code of practice for information security controls. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en. (Accessed July 2023).

iDirect, 2023. Idirect - 9350 satellite modem. https://www.idirect.net/products/9350-satellite-modem/. (Accessed July 2023).

Ivancic, W., Griner, J., Dimond, R., Frantz, B., Kachmar, B., Shell, D., 2000. Satellite communications using commercial protocols. In: 18th International Communications Satellite Systems Conference and Exhibit, p. 1185.

Jacobs, B., 2023. A comparative study of eu and us regulatory approaches to cybersecurity in space. Air Space Law 48.

Jegham, N., Beylot, A.-L., Lohier, S., Roussel, G., 2008. Performance of voice over ip in dvb-rcs and idirect satellite networks. In: 26th International Communications Satellite Systems Conference (ICSSC), pp. 1–11.

Kapalidis, C., Maple, C., Bradbury, M., Farrell, M., Fisher, M., 2019. Cyber risk management in satellite systems. In: Living in the Internet of Things (IoT 2019). IET, pp. 1–8.

Kaplan, E.D., Hegarty, C., 2017. Understanding GPS/GNSS: Principles and Applications. Artech House.

Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O., Tatar, U., 2021. Cyber third-party risk management: a comparison of non-intrusive risk scoring reports. Electronics 10, 1168.

Kitchen, J.T., Coogan, D.R., Christian, K.H., 2021. The evolution of legal risks pertaining to patch management and vulnerability management. Duq. L. Rev. 59, 269.

Kodheli, O., Lagunas, E., Maturo, N., Sharma, S.K., Shankar, B., Montoya, J.F.M., Duncan, J.C.M., Spano, D., Chatzinotas, S., Kisseleff, S., et al., 2020. Satellite communications in the new space era: a survey and future challenges. IEEE Commun. Surv. Tutor. 23, 70–109.

Kolawole, M.O., 2017. Satellite Communication Engineering. CRC Press.

Korhonen, V., 2019. Future after OpenVPN and IPsec. Master's thesis. Tampere University.

Kuang, L., Jiang, C., Qian, Y., Lu, J., 2017. Terrestrial-Satellite Communication Networks: Transceivers Design and Resource Allocation. Springer.

Lautenbacher, C.C., 2006. The global Earth observation system of systems: science serving society. Space Policy 22, 8–11.

Lee, M.T., 2011. Feasibility and performance analyses of adapting ethernet-based protocols in space-based networks. In: 2011-MILCOM 2011 Military Communications Conference. IEEE, pp. 1845–1852.

Lightman, S., Suloway, T., Brule, J., 2022. Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control. NISTIR NISTIR 8401 National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8401.

Maurushat, A., Nguyen, K., 2022. The legal obligation to provide timely security patching and automatic updates. Int. Cybersecurity Law Rev. 3, 437–465.

McLaughlin Jr, R.D., 2011. Leveraging an SNMP agent in terminal equipment for network monitoring of US Navy SATCOM. Technical Report, Naval Postgraduate School Monterey CA.

Mitra, M., 2005. Satellite Communication. PHI Learning Pvt. Ltd.

ModZero, 2020. CVE-2020-11549, Available online at https://www.cvedetails.com/cve/CVE-2020-11549/. (Accessed July 2023).

National Institute of Standards and Technology, 2001. FIPS 197: Federal Information Processing Standards Publication - Advanced Encryption Standard (AES), FIPS FIPS 197. Information Technology Laboratory, Gaithersburg. https://doi.org/10.6028/NIST.FIPS.197-upd. MD 20899-8900, Updated May 9, 2023.

National Institute of Standards and Technology, 2015. FIPS PUB 180-4: Federal Information Processing Standards Publication – Secure Hash Standard (SHS), FIPS FIPS PUB 180-4. Information Technology Laboratory, Gaithersburg. https://doi.org/10.6028/NIST.FIPS.180-4. MD 20899-8900.

National Institute of Standards and Technology, 2019. NIST SP 800-131A rev2, Technical Report National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final.

National Security Agency, 2022a. Cybersecurity Advisory: Protecting VSAT Communications. Technical Report U/OO/106122-22 | PP-22-0085, Version 1. National Security Agency.

National Security Agency, 2022b. Network Infrastructure Security Guide. Cybersecurity Technical Report U/OO/118623-22, National Security Agency, PP-22-0293 Version 1.1.

NIST, 2020a. CVE-2020-15778, national vulnerability database (NVD). https://nvd.nist.gov/vuln/detail/CVE-2020-15778.

NIST, 2020b. NIST SP 800-56A rev3, Technical Report National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final.

NIST, 2022. CVE-2022-31813, national vulnerability database. https://nvd.nist.gov/vuln/detail/CVE-2022-31813.

Olivero, G., 2022. Asset Discovery Tools Supporting Cybersecurity Inventory. Master Degree Thesis. Politecnico di Torino.

Peeters, W., 2022. Cyberattacks on satellites: an underestimated political threat, LSE IDEAS. https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

Pelton, J.N., 1994. Strategic Role of Satellites in 21st Century Information Highways. Coupling Technology to National Need, vol. 2102. SPIE, pp. 85–96.

Piez, Wendell, 2019. The open security controls assessment language (OSCAL): schema and metaschema, 23. In: Proceedings of Balisage: The Markup Conference. Rockville, MD. https://doi.org/10.4242/BalisageVol23.Piez01.

PwC, 2020. Market perspectives of ground segment as a service (gsaas). https://www.pwc.fr/fr/assets/files/pdf/2020/11/en-France-pwc-space-practice-research-paper-gsaas.pdf. (Accessed July 2023).

Qu, Z., Zhang, G., Cao, H., Xie, J., 2017. Leo satellite constellation for Internet of things. IEEE Access 5, 18391–18401.

Rasner, G.C., 2021. Cybersecurity and Third-Party Risk: Third Party Threat Hunting. John Wiley & Sons.

Ray, K., Selvamurthy, W., 2023. Starlink's role in Ukraine. J. Def. Stud. 17, 25–44.

Rementeria, S., 2022. Power dynamics in the age of space commercialisation. Space Policy 60, 101472.

Reuters, 2022. Exclusive: U.S. spy agency probes sabotage of satellite Internet during Russian cyberattack. https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/. (Accessed July 2023).

Reversemode, 2022. VIASAT incident: from speculation to technical details. https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html. (Accessed July 2023).

Ruben Santamarta, 2013. CVE-2013-6035, Available online at https://www.cvedetails.com/cve/CVE-2013-6035/. (Accessed July 2023).

S. C. on Homeland Security, G. Affairs, 2023. S. 1425, satellite cybersecurity act. https://www.cbo.gov/publication/59203.

Saeed, N., Almorad, H., Dahrouj, H., Al-Naffouri, T.Y., Shamma, J.S., Alouini, M.-S., 2021. Point-to-point communication in integrated satellite-aerial 6g networks: state-of-the-art and future challenges. IEEE Open J. Commun. Soc. 2, 1505–1525.

Santamarta, R., 2018. Last Call for SATCOM Security, IOActive. Seattle, WA.

Satellite Today, 2013. Axiros, ViaSat to produce first deployment of TR-069 protocol over a satellite network. https://www.satellitetoday.com/telecom/2013/10/04/axiros-viasat-to-produce-first-deployment-of-tr-069-protocol-over-a-satellite-network/. (Accessed July 2023).

Scholl, M., Suloway, T., 2022. NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft). Technical Report NISTIR 8270. National Institute of Standards and Technology (NIST).
Shah, S.M.J., Nasir, A., Ahmed, H., 2014. A survey paper on security issues in satellite communication network infrastructure. Int. J. Eng. Res. Gen. Sci. 2, 887–900.
Smailes, J., Salkield, E., Köhler, S., Birnbach, S., Martinovic, I., 2023. Dishing out DoS: how to disable and secure the Starlink user terminal. arXiv:2303.00582.
Space Industry Office, 2019. Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry (METI), Cybersecurity guidelines for commercial space systems.
Space Systems Command, 2022. Press Release: SSC CSCO Reaches Critical Milestone for IA-Pre, Roll-Out Begins Today. Office of Public Affairs (SSC/PA), 483 N. Aviation Blvd., El Segundo, Calif. 90245-2808.
Starlink, 2023. Bugcrowd - spacex. https://bugcrowd.com/spacex. (Accessed 10 December 2023).
Stroikos, D., 2023. China and India as rising powers and the militarisation of space. In: The Militarization of European Space Policy. Routledge, pp. 170–188.
Techq, 2022. Thousands of Internet users go dark in Europe from 'cyberattack'. https://techhq.com/2022/03/cyberattack-knocks-thousands-offline-in-Europe/. (Accessed July 2023).
Tedeschi, P., Sciancalepore, S., Di Pietro, R., 2022. Satellite-based communications security: a survey of threats, solutions, and research challenges. Comput. Netw., 109246.
United Nations, 1984. The United Nations Treaties on Outer Space. United Nations, New York.
United Nations Office for Outer Space Affairs (UNOOSA) 2023., Index of objects launched into outer space. https://www.unoosa.org/oosa/osoindex/index.jspx?lf_id=. (Accessed July 2023).
Union of Concerned Scientists, 2023. Satellite database. https://www.ucsusa.org/resources/satellite-database. (Accessed July 2023).
United Nations Office for Outer Space Affairs (UNOOSA), 2023. Un office for outer space affairs and United Kingdom launch new partnership on registering space objects. https://www.unoosa.org/oosa/en/informationfor/media/2022-unis-os-574.html. (Accessed July 2023).
Varadharajan, V., Suri, N., 2022. Security challenges when space merges with cyberspace. arXiv preprint. arXiv:2207.10798.
Viasat, 2023. 10-k viasat annual report - may 22, 2023, access the annual report via viasat investor relations. https://investors.viasat.com/sec-filings/sec-filing/10-k/0000950170-23-023444. (Accessed 14 December 2023).
Viasat News Blog, 2022. Ka-Sat network cyber attack overview. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. (Accessed July 2023).
Waedt, K., Ciriello, A., Parekh, M., Bajramovic, E., 2016. Automatic assets identification for smart cities: prerequisites for cybersecurity risk assessments. In: 2016 IEEE International Smart Cities Conference (ISC2). IEEE, pp. 1–6.
Wu, Z., et al., 2020. Spoofing and anti-spoofing technologies of global navigation satellite system: a survey. IEEE Access 8, 165444–165496.
Wysocarski, J., Narula-Tam, A., Wang, M.-C., Kingsbury, R., 2007. Integrating cots routers into terminals for future protected satcom systems with dynamic resource allocation. In: MILCOM 2007-IEEE Military Communications Conference. IEEE, pp. 1–7.
Yadav, A., Agarwal, M., Agarwal, S., Verma, S., 2022. Internet from space anywhere and anytime-starlink. Available at SSRN 4160260.
Y.E.E.S. Space, 2023. Yeess position paper on the eu space law. https://assets-global.website-files.com/62bae3239452bd3075697031/656ee68eb03257d6ab9233cc_YEESS%20position%20on%20EU%20space%20law.pdf. Submitted as an attachment to the targeted and public consultation on the EU Space Law, Brussels, 28 November, 2023.
Zero Science Lab, 2016. ZSL-2016-5359, Available online at https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5359.php. (Accessed July 2023).
Zero Science Lab, 2023. CVE-2023-22971, Available online at https://nvd.nist.gov/vuln/detail/CVE-2023-22971. (Accessed July 2023).
Zhan, Y., et al., 2020. Challenges and solutions for the satellite tracking, telemetry, and command system. IEEE Wirel. Commun. 27, 12–18.

Francesco Casaril is a doctoral student in cybersecurity at the IMT School for Advanced Studies Lucca. He is a International and Political Science graduate with a special interest in critical infrastructure security. He has a professional background in the space sector working in Brussels for a trade association representing more than 130 space companies. His research interests concern the cybersecurity dimension of space infrastructure. His PhD research focuses on SATCOM technologies and, in particular, on satellite networks and router security in view of IRIS^2, the new European flagship project for resilient space communication.

Letterio Galletta is Assistant Professor with IMT School for Advanced Studies Lucca. Previously, he was a postdoc with the Department of Computer Science, University of Pisa. His research activity mainly focuses on language-based security, i.e., using techniques from programming languages, compilers and formal verification to address security problems. He applied these techniques to different fields like adaptive software, the Internet of Things, and more recently, secure compilation, firewalls and smart contracts.