SoK: Space Infrastructures Vulnerabilities, Attacks and Defenses

Jose Luis Castanon Remy, Ekzhin Ear, Caleb Chang, Antonia Feffer, and Shouhuai Xu
{*jcastano, eear, cchang, afeffer2, sxu*}*@uccs.edu*
Laboratory for Cybersecurity Dynamics, Department of Computer Science, University of Colorado Colorado Springs

2025 IEEE Symposium on Security and Privacy (SP) | 979-8-3315-2236-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/SP61157.2025.00138

Abstract—**Space infrastructures are becoming increasingly important to the global society and economy. However, their cybersecurity is understudied despite previous endeavors. This motivates the present SoK, which is based on a novel methodology of five elements: space infrastructures model, missions, vulnerabilities, attacks, and defenses. The methodology establishes an "anatomy" of space infrastructures via the innovative notions of *mission control flows* and *mission data flows*, which are respectively inspired by the notions of control flows and data flows in program analysis. We show how the space infrastructure vulnerabilities, attacks, and defenses studied in the literature can be mapped to space mission control flows and mission data flows, leading to insights such as: *improper memory allocation* and *lack of authentication* are the two most exploited vulnerabilities reported; Global Navigation Satellite Systems (GNSS) security is most studied, mainly via physical layer security; and the most effective approach to attack the space segment is to pivot through the ground segment.**

1. Introduction

Space infrastructures, including user, ground, link, and space segments, are becoming an increasingly important domain that is critical to the global society and economy. For example, the Space Foundation estimates the global space economy in 2021 was worth US$469B [1] and the global economy will reach US$800B by 2027 (or an annual 8% growth) [2]. Despite its clear importance, the topic of space infrastructures cybersecurity is under-investigated, perhaps because space infrastructures and systems are largely proprietary, classified, or implicitly assumed to be operated by trusted entities with highly technical skill sets.

This phenomenon is a *deja vu* of what the cybersecurity community has encountered in the past: Internet was designed with the mindset for use by *trusted* users (i.e., there are no attackers), but its later wide use by the public made it necessary to secure cyberspace. We anticipate that in order for space infrastructures to achieve its potential in (e.g.) enabling the global economy, they will inevitably be open to many entities (including malicious ones) and thus it is imperative to protect them from cyber attacks. This is because the private sector, as evidenced by SpaceX, is likely to become the primary enabler of space economy.

Despite the many studies on space cybersecurity (e.g., [3–6] and the references therein) and even surveys [3, 7–14], there is still a lack of a unified view of the space cybersecurity landscape, as evidenced in this paper. This view is critical to understanding the challenges and guiding future research endeavors. This motivates the present study.

Our Contributions. This SoK makes two contributions. First, we propose an "anatomy" of space infrastructures, including: (i) a systematic model for describing user, ground, link, and space segments via three levels of abstraction (top-to-bottom): *mission* vs. *segment* vs. *component*, where each component in a segment consists of multiple *modules*; (ii) representative space missions, including *infrastructure-level* and *application-level* missions; and (iii) models of mission *control flows* and *data flows* at the granularity of *modules*. These can collectively serve as a unified way for studying space missions, vulnerabilities, attacks, and defenses.

Second, we leverage the space infrastructure anatomy to systematize space missions, including their control flows and data flows, as well as the cyber vulnerabilities, attacks, and defenses described in 87 publications we identified. This leads to interesting findings, including: (i) *improper memory allocation* and *lack of authentication* are the two most exploited vulnerabilities in space infrastructure attacks; (ii) the Positioning, Navigation, and Timing (PNT) broadcast data flow has been attacked most, perhaps because researchers only need to use low-cost software defined radios and exploit the *lack of authentication* vulnerability; (iii) Global Navigation Satellite Systems (GNSS) security is most studied, mainly via physical layer security mechanisms; and (iv) the most effective approach to attacking the space segment is to pivot through the ground segment, highlighting the importance of hardening ground segment security.

Related Work. There are surveys/SoKs on space cybersecurity, which can be classified into three categories. The first category focuses on *communications* security, including: (i) physical layer security of space systems in non-geostationary orbits, summarizing security metrics for ground-to-satellite communications [8]; (ii) physical layer security for three kinds of communication channels, namely those between users and satellites without terrestrial relays, those between users and satellites via terrestrial relays, and those between satellites and terrestrial networks [9]; and (iii) preventive and reactive defenses against physical layer attacks, including eavesdropping, jamming, spoofing, and impersonation [11]. The second category focuses on *PNT* security, including: (i) spoofing attacks against GNSS [7]; (ii) navigation signal spoofing attacks as well as preventive and reactive defenses against them [12]; (iii) cryptographic navigation signal authentication schemes in the context of

DOI 10.1109/SP61157.2025.00138

the Global Positioning System (GPS) and the BeiDou Navigation Satellite System [13]; and (iv) navigation message authentication for BeiDou [14]. The third category focuses on *space systems* security, including: (i) characterizing attacks against, and defenses for, space systems via satellite signal, space platform, and ground system attack surfaces [3]; (ii) attacks against, and defenses for, integrated space-air-ground-sea networks [10]; and (iii) systematizing public key infrastructure-enabled trust and terrestrial user location privacy in space-enabled service networks [15].

By contrast, we propose a space infrastructures anatomy, which can serve as a baseline for casting space cybersecurity research into a unified view. Figure 1 summarizes the difference between the studies mentioned above and ours.

Papers	Missions				Segment-based Vulnerabilities, Attacks, and Defenses			
	Bus Mgmt.	Com ms.	PNT	Sci.	User	Ground	Link	Space
[7] (2016)			✓		1A, 5D*		3A*	
[8] (2018)		✓				2D		
[9] (2019)						3D*		
[10] (2021)			✓			2A, 1D	4A, 1D	1A, 2D
[11] (2022)					1D			4A
[12] (2022)			✓		2A*, 7D		3A*	
[3] (2022)						1A*, 3D	1A*	1A*, 3D
[13] (2023)			✓		2D			
[14] (2023)			✓		1A, 2D*		1A	
[15] (2024)		✓			1D*	7D*		7D*
This Paper	✓	✓	✓	✓	3V, 11A, 43D	3V, 4A, 5D	5A, 5D	11V, 5A, 9D

Figure 1: Comparison between previous studies and ours through the lens of space missions, vulnerabilities (e.g., 3V means 3 vulnerabilities covered in a study), attacks (e.g., 4A means 4 attacks), defenses (e.g., 2D means 2 defenses), and * indicates the number of attack categories (e.g., 2A* means two categories of attacks) and defense categories (e.g., 7D*).

Paper Outline. Section 2 presents our systematization methodology. Section 3 describes our space infrastructures model. Section 4 discusses space missions. Sections 5-7 respectively systematizes space cyber vulnerabilities, attacks, and defenses. Section 8 discusses the relationships between missions, vulnerabilities, attacks and defenses, as well as future research directions. Section 9 concludes the paper.

2. Systematization Methodology

Scope. We focus on systematizing academic literature because they provide the due technical details. We exclude space incidents briefly reported in social media such as blogs, non-technical news sources because they do not provide technical details, and industry sources because they are often proprietary/classified. We refer to [4, 6] for "'hypothetical" analyses of real-world space cyber attacks whose technical details are often missing.

Methodology. Figure 2 highlights our methodology, which is composed of: (i) *space infrastructures model*, (ii) *missions*, (iii) *vulnerabilities*, (iv) *attacks*, and (v) *defenses*. The space infrastructures model represents the anatomy of space systems and networks. We describe this anatomy at three levels of abstraction: *missions*, namely, the operations that enable and accomplish the services provided by space infrastructures; *segments*, namely user, ground, link, and space; and *components*, namely the components of each segment where each component consists of multiple *modules*.

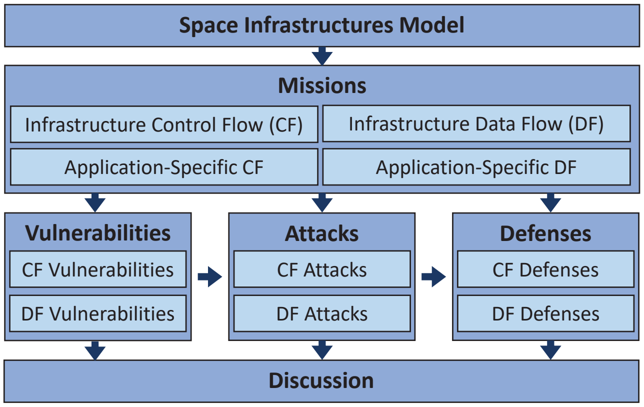

Figure 2: Systematization methodology.

The anatomy paves a way for introducing two important concepts: mission *control flows* (CF), which describe the processes whereby space systems are controlled, and mission *data flows* (DF), which describe the processes whereby data is generated, transmitted and processed. They are described at two levels: infrastructure-level CFs and DFs, which are associated with the operation of a space infrastructure; application-level CFs and DFs, which are specific to each application (e.g., services provided by satellites). These concepts are inspired by the notions of control flows and data flows in program analysis, but are at a higher level of abstraction in the context of space infrastructures.

The anatomy and the CF/DF concepts allow us to systematize space infrastructures' cyber vulnerabilities, attacks, and defenses described in the literature, as follows. First, we systematize vulnerabilities with respect to the vulnerable modules in CFs and DFs, helping understand the exploitation points and potential impacts. Second, we systematize attacks based on how they affect CFs and DFs, helping understand the impacts of attacks on missions. Third, we systematize defenses based on where they are applied to harden CFs and DFs from attacks. Fourth, we map between missions, vulnerabilities, attacks, and defenses to provide a holistic view, highlighting which missions have which vulnerabilities, that can be exploited by which attacks, that can be mitigated by which defenses. Fifth, we discuss future research directions toward hardening space cybersecurity.

Literature Search. For systematization purposes, we use Google Scholar to identify relevant literature published during 2013-2023 in the following venues: ACM CCS, IEEE SP, Usenix Security, NDSS, ACM AsiaCCS, ACSAC, RAID, ACM Computing Survey, IEEE Survey and Tutorials on Communication, IEEE T-IFS, IEEE TDSC, ACM TOPS, PLANS, AERO, IEEE Transactions on Aerospace and Electronic Systems, International Conference on Wireless and Mobile Computing (WiMob) and ION GNSS+.

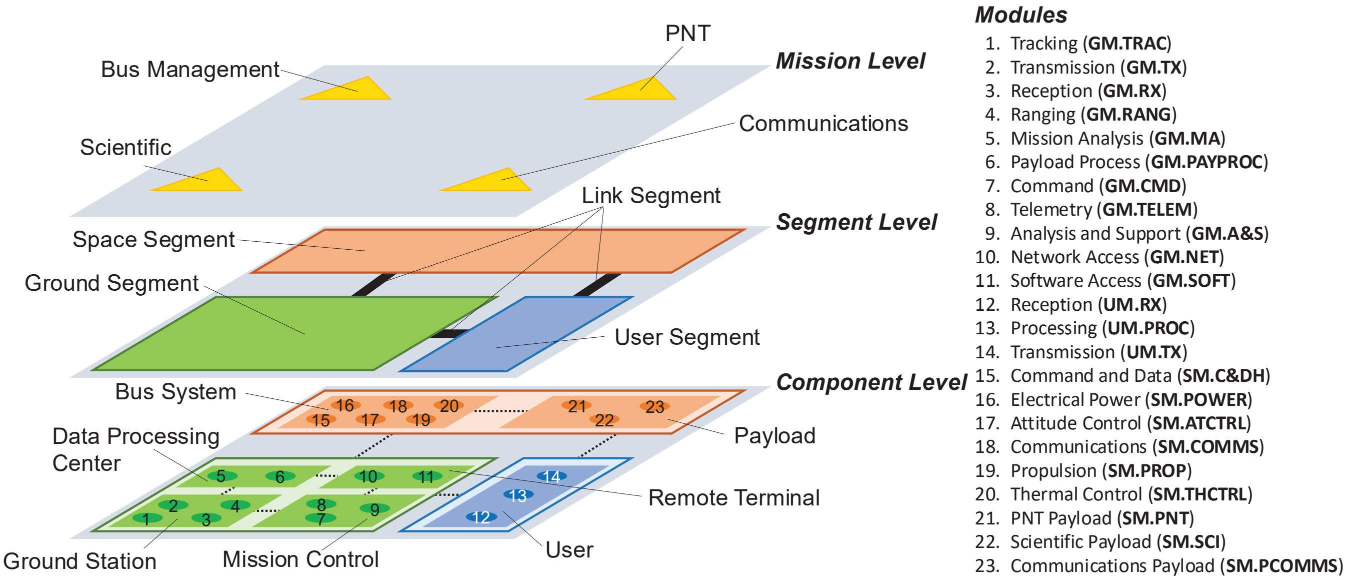

Figure 3: Space infrastructures model with three levels of abstraction (i.e., mission, segment, component), where a component consists of multiple modules which are numbered and referred to as such. Note that modules in different segments can have the same name because they have the same functionality, and we differentiate them via the following module acronyms convention: prefix indicates the segment to which the module belongs (e.g., GM indicates Ground segment Module).

We select the preceding venues because they are major security venues or we are aware of relevant papers published in a non-security venue. Since Google Scholar limits the number of keywords in a single search, we perform two queries. The first query uses keywords "space security" OR "space threats" OR "space vulnerability" OR "space architecture" OR "space cybersecurity" OR "space defense" OR "space attack" OR "satellite security." The second query uses keywords "GNSS spoofing" OR "jamming attack" OR "anti-jamming" OR "anti-spoofing." From the outcome of the two queries, we select 518 unique papers based on their titles. By manually reviewing each paper's technical relevance to space cyber vulnerability, attack, or defense, we identify 87 papers to systematize.

3. Modeling Space Infrastructures

Overview. Figure 3 highlights the model with three levels of abstraction: *mission level*, which describes the operations that maintain a space infrastructure or enable the services or applications it provides; *segment level*, which has four segments (i.e., user, ground, link, and space); and *component* level, where a component resides inside a segment, and *modules* reside in a component. Note that module is the finest granularity in the present paper, and that segments, components, and modules formulate a hierarchical structure (i.e., a segment consists of components and a component consists of modules). Also as highlighted in Figure 3, we use the following acronym convention for modules: XM.module_name, where $X \in \{\mathrm{U}, \mathrm{G}, \mathrm{L}, \mathrm{S}\}$ representing segment. For instance, GM.TRAC indicates the *tracking* module in the ground segment.

User Segment (U). As shown in Figure 3, the user segment has a *user* component, which is an end user of services provided or enabled by a space infrastructure. This component is typically terrestrially stationed and consists of three modules: (i) The *transmission* module, UM.TX, sends data from the user to a satellite or a ground relay, such as voice transmission over satellite communications (SATCOM). The speed and amount of data transmitted depend on user requirements and satellite capability because some satellites do not have the capability to receive user transmissions, as in the case of GNSS. (ii) The *reception* module, UM.RX, receives data from a satellite or ground relay via UM.TX. Typically, users receive broadcast messages from a satellite via line-of-sight transmission. The received data may be bursty as in the case of SATCOM, or steady as in the case of GNSS. (iii) The *processing* module, UM.PROC, processes the data received from a satellite or ground relay (via UM.RX) for mission purposes (e.g., decompressing a SATCOM video stream).

Ground Segment (G). As shown in Figure 3, the ground segment has four components: *ground station*, *data processing center*, *mission control*, and *remote terminal*. These four components are terrestrially stationed, and support both the space segment and the user segment.

A *ground station* component includes the hardware and software that are needed to establish communication channels with satellites. This component consists of four modules: (i) The *tracking* module, GM.TRAC, monitors satellites' orbits such as position, orientation, and trajectory. (ii) The *transmission* module, GM.TX, physically transmits Radio Frequency (RF) signals to satellites. (iii) The *reception* module, GM.RX, physically receives RF signals from satellites. (iv) The *ranging* module, GM.RANG, attains measurements of the distance and direction from the ground station to satellites and other space objects (e.g., debris).

A *data processing center* component analyzes payload data collected by the space segment, namely the data produced by, or associated with, the missions executed by satellites. This component consists of two modules: (i) The *mission analysis* module, GM.MA, processes data related to the mission of a satellite (e.g., processing data related to the orbit of a satellite to assess whether the current orbit lets the satellite achieve the mission). (ii) The *payload process* module, GM.PAYPROC, processes data directly generated by the payload component of the satellite (e.g., processing images from the Earth's atmosphere taken by the *payload* component of the satellite, which is described below). A *data processing center* is computationally powerful.

A *mission control* component commands the satellite, and receives and analyzes telemetry data (e.g., electrical power, battery levels, orbital velocity, altitude, position, propellant levels and temperature) collected by the *electrical power* module SM.POWER, the *attitude control* module SM.ATCTRL, and the *thermal control* module SM.THCTRL. This component consists of three modules: (i) the *command* module GM.CMD, which produces commands to control the space segment; (ii) the *telemetry* module GM.TELEM, which analyzes infrastructure-level mission data (i.e., telemetry data from the *telemetry* module); and (iii) the *analysis and support* module GM.A&S, which analyzes application-level mission data (i.e., from modules in the payload component) and provides additional support for the *command* module GM.CMD.

A *remote terminal* component includes a hardware and software stack whereby operators remotely access the other components of the ground and space segments. It has two modules: (i) the *network access* module GM.NET, which provides operators with remote accesses to network enclaves in the ground segment, such as the command module GM.CMD (for issuing flight commands); (ii) the *software access* module GM.SOFT, which provides operators with software services in the ground segment, such as flight and orbit simulation in the *mission analysis* module GM.MA.

Link Segment (L). As shown in Figure 3, the link segment corresponds to the data connections between the components in the same or different segments. We refer to communications between different segments as *inter-segment links* and communications within a single segment as *intra-segment links*. Inter-segment links from the ground and user segments to the space segment are referred to as *uplinks*; transmissions from the space segment to the ground and user segments are referred to as *downlinks*; transmissions between satellites are referred to as *crosslinks*. Uplinks and downlinks are typically used for managing and commanding satellites, communicating users, and accomplishing missions of satellites (e.g., delivering their services). These links typically use RF signals in the shape of a cone, beam or footprint, which can travel vast distances. Uplinks and certain downlink transmissions (e.g., satellite to ground stations) signals are shaped into a narrow beam, leading to strong signals. On the other hand, downlink transmission (e.g., satellite to users in the user segment) signals tend to be broadcasted across large areas (e.g., a cone under the sending satellite) as communications satellites must transmit to many users simultaneously, where the strength of the signal is decreased. By contrast, intra-segment links are typically used for coordination of efforts and other logistical and administrative requirements. These links are typically wired connections, which travel short distances or leverage Internet-based networks.

Space Segment (S). As shown in Figure 3, the space segment (e.g., the satellite) has two components, *bus system* and *payload*. The *bus system* component is in charge of the control of a satellite and fulfills infrastructure-level missions and thus supports application-level missions, similar to operating systems (OS) supporting applications. This component consist of six modules. (i) The *command and data* module SM.C&DH receives and processes commands from the ground segment *command* module GM.CMD. (ii) The *electrical power* module SM.POWER controls the production and distribution of electrical power that is needed by the other modules (e.g., controlling the solar panels to generate solar energy). (iii) The *attitude control* module SM.ATCTRL controls the orientation of a satellite relative to the body being orbited. (iv) The *communications* module SM.COMMS connects (i.e., through radio hardware) the bus system to the *transmission* module GM.TX and the *reception* module GM.RX. (v) The *propulsion* module SM.PROP controls the components that propel the satellite. (vi) The *thermal control* module SM.THCTRL monitors and controls the temperature of the satellite.

A *payload* component fulfills an application-level mission. It has three modules. (i) The *positioning, navigation, and timing (PNT) payload* module SM.PNT provides GNSS services, such as GPS and BeiDou. (ii) The *scientific payload* module SM.SCI enables scientific and remote sensing missions (e.g., sensors to monitor space weather, or zero-gravity experiment and testing). (iii) The *communications payload* module SM.PCOMMS provides terrestrial voice, video, and data connections (e.g., antennas).

4. Missions

As highlighted in Figure 3, we focus on four missions: (i) bus management, which is realized by the *bus system* component that operates and maintains satellites; (ii) communications, which is realized by the *communications* module SM.COMMS; (iii) PNT, which is realized by the *PNT* module SM.PNT; and (iv) scientific, which is realized by the *scientific* module SM.SCI. Note that (i) is an infrastructure-level mission and (ii)-(iv) are application-level missions. A mission may cut across multiple segments via its CFs and DFs. In principle, CFs and DFs are graphs, where nodes represent modules in Figure 3 and arcs represent the flows of commands or data. Similar to the acronym convention for modules, we use CF.NAME (DF.NAME) to name and refer to control (data) flows.

4.1. Bus Management Mission

This mission is for satellite operators to manage and control a satellite. For instance, the ground segment receives and processes telemetry data from the *bus system* component of a satellite, and then decides and communicates commands to the *bus system* component to maneuver the satellite to avoid conjunctions (i.e., collisions). This mission has two CFs and two DFs.

4.1.1. Bus Management Control Flow (CF.BUSM). This CF describes the process that produces and delivers a command to the *bus system* component. As highlighted in Figure 4, this CF cuts across the ground and space segments (coded in color and indicated by the prefixes of module identifiers). It has nine nodes in total and is elaborated below.

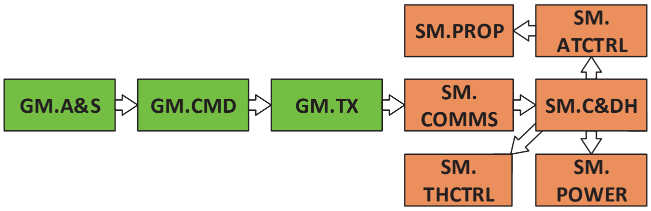

Figure 4: Bus management control flow (CF.BUSM)

(i) The CF originates at the *analysis and support* module GM.A&S, which analyzes the telemetry and relevant mission data and outputs a decision, such as maneuvering the satellite to avoid a conjunction, correcting the satellite's orbit, or adjusting the temperature and/or energy consumption in the satellite. (ii) The *command* module GM.CMD receives the decision and produces a command accordingly, such as a flight command for maneuvering the satellite or a management command for adjusting the temperature and/or energy consumption in the satellite. (iii) The *transmission* module GM.TX receives, processes and encodes the command into a digital signal, which is then modulated into a RF signal. (iv) The *transmission* module GM.TX transmits the RF signal to the *communications* module SM.COMMS in the space segment once the two modules' antennas are in line of sight of each other. (v) The *command and data* module SM.C&DH receives the RF signal, demodulates it into a digital signal, which is then decoded to obtain the command. The command is sent to the intended module, such as the *thermal control* module SM.THCTRL or the *electrical power* module SM.POWER for a management command, or the *attitude control* module SM.ATCTRL for a flight command. (vi) The *thermal control* module SM.THCTRL receives a management command and then adjusts the temperature of the satellite as instructed. (vii) The *electrical power* module SM.POWER receives a management command and adjusts the energy consumption in the satellite as instructed. Note that some satellites include a Battery Management System (BMS), which autonomously manages the energy consumption in the satellite (e.g., powering off non-critical modules when the battery reaches a certain threshold). For instance, when the battery is below 20%, the BMS can power off modules in the space segment other than the *command and data* module SM.C&DH and the *electrical power* module SM.POWER until the battery is fully charged. (viii) The *attitude control* module SM.ATCTRL receives a flight command, which instructs the *propulsion* module SM.PROP to maneuver the satellite.

4.1.2. Remote Management Control Flow (CF.REMM). This CF describes how ground operators access ground segment functions remotely. As highlighted in Figure 5, this CF is within the ground segment. It has seven nodes in total and is elaborated below. (i) The CF originates at the *software access* module GM.SOFT, which hosts an application service that is used by a ground operator (e.g., through a computer running a VPN access). This module prepares the parameters for establishing a connection between the remote human operator and the desired module the operator needs to connect with (e.g., *mission analysis* GM.MA). (ii) The *network access* module GM.NET receives the connection parameters and establishes a connection between the remote human operator and the desired module the operator intends to control. The network hardware (e.g., router) in the *network access* module GM.NET connects the *software access* module GM.SOFT to the *mission analysis* module GM.MA, the *payload process* module GM.PAYPROC, the *command* module GM.CMD, the *telemetry* module GM.TELEM, or the *analysis and support* module GM.A&S through the Internet or private ground networks, allowing the human operator remote access to mission analysis, payload management, bus management, telemetry collection, or mission control functions.

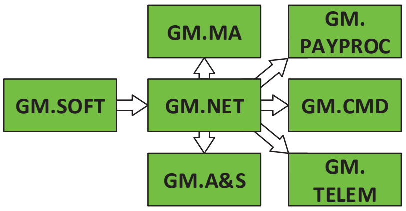

Figure 5: Remote management control flow (CF.REMM)

4.1.3. Telemetry Reporting and Analysis Data Flow (DF.TELEM). This DF describes how telemetry data is generated, transmitted and processed throughout a space infrastructure (i.e., from the *bus system* component in the space segment to the *mission control* component in the ground segment). Telemetry data provides *condition reports* on the health of a satellite and *status reports* on the operational state of a satellite (i.e., being able to receive and execute commands and provide outputs). This DF is activated at regular time intervals or on-demand. As shown in Figure 6, this CF has eight nodes in total and is elaborated below.

(i) The DF originates at the *electrical power* module SM.POWER, the *attitude control* module SM.ATCTRL, or the *thermal control* module SM.THCTRL, which generate telemetry data. (ii) The *command and data* module SM.C&DH receives the telemetry data and crafts a data packet. (iii) The *communications* module SM.COMMS receives the data packet, processes it, and modulates the data

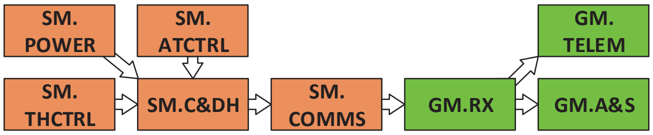

Figure 6: Telemetry reporting and analysis (DF.TELEM)

into a RF signal, which is transmitted to the *reception* module GM.RX whenever the former is within the downlink footprint of the satellite (i.e., within range of the satellite's reception antennas). (iv) The *reception* module GM.RX receives the RF signal and demodulates it to digital telemetry data. (v) The *telemetry* module GM.TELEM receives the telemetry data, where a human operator monitors the health condition of the satellite. (vi) The *analysis and support* module GM.A&S receives the telemetry data, and then a human operator extracts the location data from the telemetry data and update the space situational awareness (SSA) repository.

4.1.4. Orbit Management Data Flow (DF.ORBM). This DF describes how human operators in the ground segment can obtain orbital parameters of satellites and then update the ephemeris data, which includes position, time, velocity, and coordinate system information of a satellite. As shown in Figure 7, this DF is within the ground segment, has four nodes, and is elaborated below. (i) This DF originates at the *tracking* module GM.TRAC, the *ranging* module GM.RANG, or the *analysis and support* module GM.A&S, where orbital parameters of the satellite are obtained. Specifically, GM.TRAC collects and calculates azimuth, elevation, and antenna position data, for which we refer to [16] for details; GM.RANG collects and calculates time-of-flight, atmospheric observation, and signal related data [16]; GM.A&S collects data from the SSA repository of state vectors for the satellite in question. (ii) The *mission analysis* module GM.MA receives the data from the preceding modules, and informs the operator to make a decision on the mission satellite's orbit.

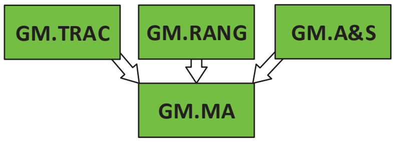

Figure 7: Orbit management data flow (DF.ORBM)

4.2. Communications Mission

Space infrastructures enable user-to-user and user-to-network communications especially in the absence of traditional telecommunication, wireless, or terrestrial Internet services. Space-enabled communications are often characterized by their bandwidth, frequency modulation, and latency, all of which may be impacted by atmospheric attenuation, weather conditions, and interferences. Space-enabled communications increasingly leverage satellite constellations to transmit signals or satellite networks. This mission has one CF and one DF.

4.2.1. Subscription Management Control Flow (CF.SUBSM). This CF enables an end user in the user segment to establish a communication channel with a communication module on a satellite. An end user subscribes to communication services, where the communication parameters need to be established (e.g., signal strength, frequency channel, and frequency modulation). As shown in Figure 8, this CF has seven nodes in total. (i) The CF originates at the *transmission* module UM.TX, which establishes the communication channel parameters via ground terrestrial communications and sends them to the *mission analysis* module GM.MA. (ii) The *mission analysis* module GM.MA receives and analyzes the parameters received. (iii) The *command* module GM.CMD receives the parameters and produces a communication command with the parameters, such as the signal strength, the frequency channel and the frequency modulation. (iv) The *transmission* module GM.TX processes and modulates the command into a RF signal. (v) The *communications* module SM.COMMS receives the RF signal and demodulates it into a command. Note that GM.TX physically transmits the RF signal to the satellite once its antenna and the antenna in SM.COMMS are in line of sight of each other. (vi) The *command and data* module SM.C&DH receives and interprets the command. (vii) The *communications payload* module SM.PCOMMS receives the command and establishes a communication channel with the user communication parameters.

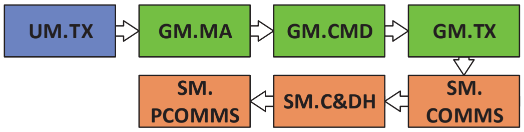

Figure 8: Subscription management (CF.SUBSM)

4.2.2. Channel Operations Data Flow (DF.CHAO). This DF describes data communications between end users via the space segment. As highlighted in Figure 9, this DF has four nodes. (i) The DF originates at the *transmission* module UM.TX, which sends data through a communication channel. (ii) The *communications payload* module SM.PCOMMS receives the data and transmits it to the end user, including ground station, assuming the end user is in the downlink footprint of the satellite; otherwise, the SM.PCOMMS uses a crosslink to transmit the data to the SM.PCOMMS of another satellite. (iii) A *reception* module, GM.RX or UM.RX, receives RF signals whenever it is in the downlink footprint of the satellite. These signals are then converted into data.

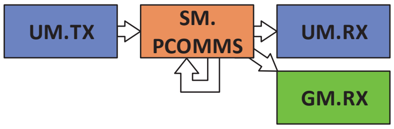

Figure 9: Channel operations data flow (DF.CHAO)

4.3. PNT Mission

Space infrastructures enable the application-level PNT mission that provides end users with time data (e.g., clock corrections) and the state vector of a PNT satellite, including its location in the form of the classical orbital elements and perturbations, while noting that perturbations are necessary corrections to the orbit because of external conditions (e.g., atmospheric drag). [16]. The end user can triangulate its position, populate its routes, or sync its clock based on three or more PNT satellites' locations and timing information, while noting that four or more satellites can lead to more accurate positioning and that positioning and navigation rely on timing to provide accurate measurements [17, 18]. This mission has one CF and one DF.

4.3.1. Time Synchronization Control Flow (CF.TIMES). This CF describes how the clock in a PNT satellite is corrected [19]. As highlighted in Figure 10, this CF has seven nodes in total. (i) The CF originates at the *mission analysis* module GM.MA, where correctness of a PNT satellite's clock is assessed. If the clock is out of synchronization, GM.MA notifies the *payload process* module GM.PAYPROC. (ii) The *payload process* module GM.PAYPROC receives the notification and calculates the correction. (iii) The *command* module GM.CMD receives the correction and produces a timing correction command. (iv) The *transmission* module GM.TX modulates the command into a RF signal. (v) The *communications* module SM.COMMS receives the RF signal and demodulates it into a command. (vi) The *command and data* module SM.C&DH receives and interprets the command. (vii) The *PNT payload* module SM.PNT receives the command and corrects the clock on the satellite.

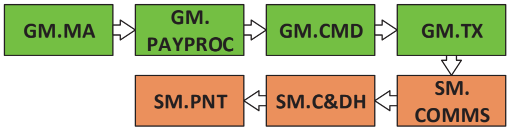

Figure 10: Time synchronization (CF.TIMES)

4.3.2. PNT Broadcast Data Flow (DF.PNT). This DF describes how users (e.g., end users or ground stations) receive position and timing data for navigation purposes. As highlighted in Figure 11, this DF has four nodes in total. (i) The DF originates at the *PNT payload* module SM.PNT, which broadcasts the position and time of the satellite via a RF signal. (ii) A *reception* module, GM.RX or UM.RX, receives and demodulates the RF signal into position and timing data. (iii) The *mission analysis* module GM.MA and the *processing* module UM.PROC use the position and timing data to compute its own positioning and navigation or correct its timing.

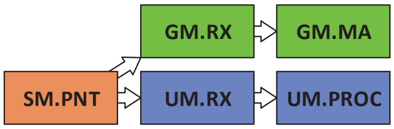

Figure 11: PNT broadcast (DF.PNT))

4.4. Scientific Mission

Space infrastructures enable application-level scientific missions, such as: (i) experiments for understanding the effects of space in various scientific fields (e.g., the effects of space travel on human body [20]; and (ii) remote sensing missions oriented toward the Earth or other celestial bodies to collect data about the planetary surface or the atmosphere. Note that remote sensing includes active and passive sensing systems: active sensors emit energy that reflects on the planet's surface or atmosphere (e.g., Earth terrain mapping, disaster management, or environmental surveillance); passive sensors measure the energy emitted by another source (e.g., from the Sun and reflected by Earth's surface). Satellites enabling scientific missions typically have uplink and downlink communications with a network of strategically located ground stations, which in turn, connect to the data processing centers that have the requisite compute resources.

4.4.1. Scientific Mission Control Flow (CF.SCI). This CF enables operators to manage and control the scientific module in the space segment. As highlighted in Figure 12, this CF has six nodes. (i) This CF originates at the *mission analysis* module GM.MA, which receives and analyzes experiment parameters that will be tested in the satellite's *scientific payload* module SM.SCI. (ii) The *command* module GM.CMD receives the experiment parameters and produces an experiment setup command. (iii) The *transmission* module GM.TX modulates the command into a RF signal. (iv) The *communications* module SM.COMMS receives the RF signal and demodulates it into a command. (v) The *command and data* module SM.C&DH receives and interprets the command. (vi) The *scientific payload* module SM.SCI receives the command and executes it.

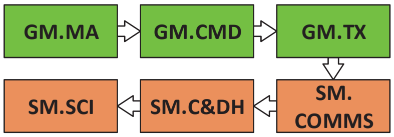

Figure 12: Scientific mission (CF.SCI))

4.4.2. Scientific Mission Data Flow (DF.SCI). This DF describes how users (e.g., end users or ground stations) receive scientific data from a satellite. As highlighted in Figure 13, it has seven nodes in total.

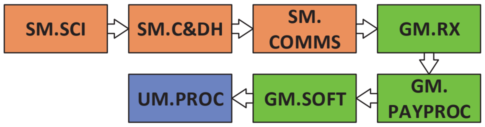

Figure 13: Scientific mission (DF.SCI)

(i) This DF originates at the *scientific payload* module SM.SCI, which produces scientific data (e.g.) from exper-

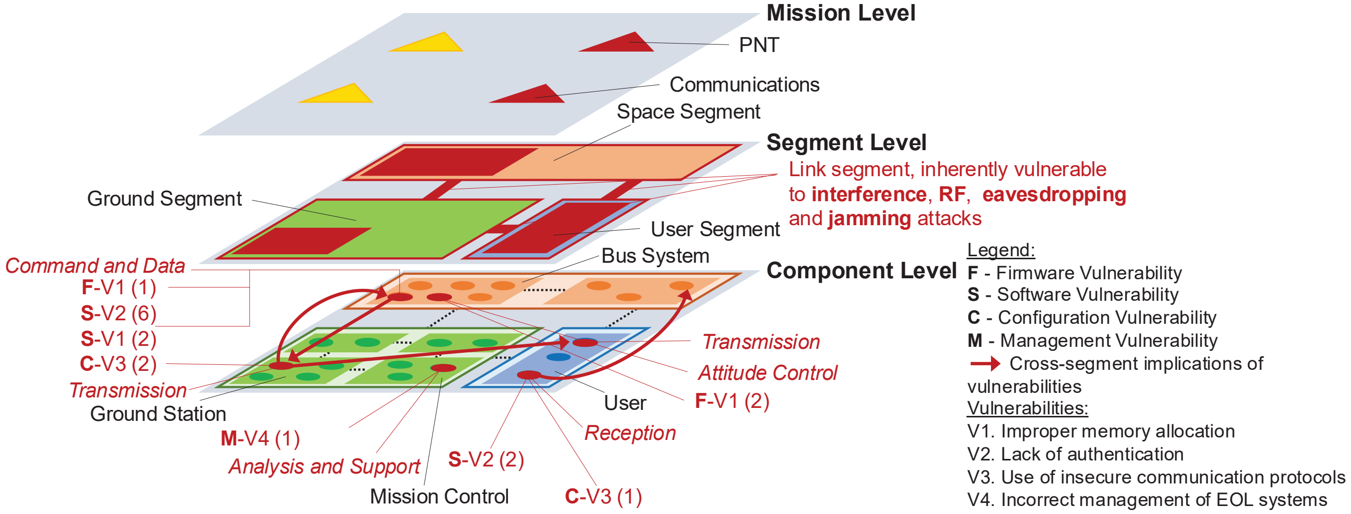
Mission Level
PNT
Communications
Space Segment
Segment Level
Link segment, inherently vulnerable
to interference, RF, eavesdropping
and jamming attacks
Ground Segment
User Segment
Bus System
Component Level
Legend:
F - Firmware Vulnerability
S - Software Vulnerability
C - Configuration Vulnerability
M - Management Vulnerability
Cross-segment implications of vulnerabilities
Vulnerabilities:
V1. Improper memory allocation
V2. Lack of authentication
V3. Use of insecure communication protocols
V4. Incorrect management of EOL systems
Command and Data
F-V1 (1)
S-V2 (6)
S-V1 (2)
C-V3 (2)
Transmission
Ground Station
M-V4 (1)
Analysis and Support
Mission Control
S-V2 (2)
C-V3 (1)
Reception
User
Transmission
Attitude Control
F-V1 (2)

Figure 14: Vulnerabilities reported in the literature and cast into the system model, where "X-Vi (j)" means j instances of vulnerability Vi of type X∈{F, S, C, M}, where $i \in \{1, \ldots, 4\}$.

iments. (ii) The *command and data* module SM.C&DH receives the scientific data and crafts a data packet. (iii) The *communications* module SM.COMMS receives the data packet, modulates the data into a RF signal, and transmits the signal to the *reception* module GM.RX whenever the GM.RX is in the downlink footprint of the satellite. (iv) The GM.RX receives the RF signal and demodulates it into scientific data. (v) The *payload process* module GM.PAYPROC receives and consumes the scientific data. (vi) The *software access* module GM.SOFT receives and hosts the processed scientific data. (vii) The *processing* module UM.PROC receives and consumes the processed scientific data.

5. Vulnerabilities

As highlighted in Figure 14, there are four known vulnerabilities, which can affect two mission CFs and five DFs. The vulnerabilities are: (V1) improper memory allocation in the space segment [21, 22]; (V2) lack of authentication [22–25]; (V3) use of insecure protocol [22, 26, 27]; and (V4) incorrect satellite end-of-life (EOL) management [28]. We map them to the CFs and DFs as follows.

5.1. Control Flow Vulnerabilities

Vulnerabilities associated with CF.BUSM. The *bus management* CF (Figure 4) has the four known vulnerabilities. (i) The *analysis and support* module GM.A&S can contain V4 (incorrect satellite EOL management), meaning it runs unpatched flight software that can be exploited by an attacker to gain control over a satellite and possibly attack the other satellites in the same constellation [28]. (ii) The *transmission* module GM.TX may contain V3 (use of insecure protocol) when rural users connect to the Internet via satellite service (and ground stations) [26], such as the use of HTTP (rather than HTTPS) or POP3 (rather than POP3S) in maritime networks [27] and the use of insecure proprietary communication protocols [22]. These vulnerabilities allow an attacker to eavesdrop the unencrypted traffic over both downlinks and uplinks. (iii) The *command and data* module SM.C&DH can contain V2 (lack of authentication) in the ground station to satellites communication protocol. This vulnerability exists in the communications between the NASA Core Flight System (cFS), which runs in satellite bus system, and the Comprehensive Open-architecture Solution for Mission Operations Systems (COSMOS), which runs in ground station [24], and can be exploited to spoof commands from ground station to control a satellite. SM.C&DH can also contain V1 (improper memory allocation), which resides in the embedded Real-time Onboard Dependable Operating System (RODOS) running in satellites and enables an attacker to send telemetry data to a vulnerable satellite to control its firmware or software [21]. (iv) The *attitude control* module SM.ATCTRL can contain V1 (improper memory allocation) in the firmware that controls this module, and the vulnerability permits attacker to control a satellite's position [22].
Vulnerabilities associated with CF.SCI. This CF (Figure 12) has two known vulnerabilities. (i) The *transmission* module GM.TX may contain V2 (lack of authentication), which can be exploited to spoof scientific commands [22, 24]. (ii) The *command and data module* SM.C&DH can contain V1 (improper memory allocation), which can be exploited by an attacker to gain control over a satellite and prevent the *scientific payload* module SM.SCI from receiving Scientific commands [21, 22].

5.2. Data Flow Vulnerabilities

Vulnerabilities associated with DF.TELEM. This DF (Figure 6) may contain three (our of the four) vulnerabilities. (i) The *attitude control* module SM.ATCTRL can contain V1 (improper memory allocation), which enables an attacker to malign telemetry data generated in this module [22]. (ii) The *command and data* module SM.C&DH, the *communications* module SM.COMMS, and the *reception* modul GM.RX can have V1 in their firmware [21] and V2 in their software [24], where an exploitation allows an attacker to prevent the *telemetry* module GM.TELEM and the *analysis and support* module GM.A&S from having access to the telemetry data, rendering operators blind to the status and health of the satellite. (iii) GM.TELEM and GM.A&S can contain V1 whereby an attacker can corrupt the processing of telemetry data [21]. (iv) The arcs in the DF can have vulnerabilities such as V3 (use of insecure protocol), which allows an attacker to disclose sensitive telemetry data [27].

Vulnerabilities associated with DF.ORBM. This DF (Figure 7) can have the following two vulnerabilities. (i) The *mission analysis* module GM.MA can contain V1 (improper memory allocation), which permits an attacker to corrupt the operator's space objects repository and thus adversely affect the space situational awareness (e.g., mis-tracking of objects, which can cause satellites conjunction) [21]. (ii) GM.A&S can have V4 (incorrect satellite EOL management), encroaching on other managed orbits [28].

Vulnerabilities associated with DF.CHAO. This DF (Figure 9) may possess three vulnerabilities. (i) The *communications payload* module SM.PCOMMS can contain V1 (improper memory allocation), which allows an attacker to compromise sensitive user data [21]. (ii) The *reception* modules, GM.RX and UM.RX, can contain V2 (lack of authentication), which allows an attacker to have access to sensitive user channel subscription data [23]. (iii) The arc "SM.PCOMMS→UM.RX" can be inherently vulnerable because of the nature of radio wave propagation and the presence of V3 (use of insecure protocol), allowing an attacker to compromise data confidentiality [27].

Vulnerabilities associated with DF.PNT. This DF (Figure 11) can contain the following two vulnerabilities. (i) The *reception* module UM.RX may contain V2 (lack of authentication), permitting an attacker to corrupt GNSS data by injecting spoofed GNSS signals to mislead users with wrong location information (e.g., drone's autonomous flight system) [23]. (ii) The *processing* module UM.PROC can have V2 (lack of authentication), allowing an attacker to attain a user's location [24]. (iii) The arc "SM.PNT→UM.RX" can contain V3 (use of insecure protocol), allowing an attacker to compromise data confidentiality [27].

Vulnerabilities associated with DF.SCI. This DF (Figure 13) has three vulnerabilities. (i) The *scientific payload* module SM.SCI can possess V1 (improper memory allocation), allowing an attacker to deny/disrupt access to research data by saturating the system's memory and crash the module [21]. (ii) The *reception* module GM.RX and the *processing* module UM.PROC can contain V2 (lack of authentication), allowing the compromise of confidentiality of scientific sensor data [25]. (iii) The *payload processing* module GM.PAYPROC and the *software access* module GM.SOFT can have V3 (use of insecure protocol), allowing data reuse and the compromise of data integrity [27]. (iv) The arc "SM.COMMS→GM.RX" contains V3, allowing an attacker to breach data confidentiality [27].

Summarizing the preceding discussion, we draw:

Insight ***1.*** The two most exploited vulnerabilities reported in the literature are *improper memory allocation* (V1) and *lack of authentication* (V2), each with six instances.

Note that Insight 1 captures some unique aspects of space cybersecurity because V1 hints insecure design and/or lack of cybersecurity testing (perhaps inherent to the closed-design nature of space systems) and V2 hints legacy space systems are not designed in a principled fashion.

6. Attacks

As highlighted in Figure 15, the following nine attacks have been reported in the literature: (A1) RF spoofing [23, 29–35]; (A2) RF replaying [36–38]; (A3) RF jamming [23, 39]; (A4) RF eavesdropping [40–42]; (A5) RF interference [43, 44]; (A6) denial of service against modules [45, 46]; (A7) data injection into Space Situational Awareness (SSA) repository [47, 48]; (A8) physical damage of satellites [49, 50]; and (A9) gaining control of satellites [46, 51]. We map them to the CFs and DFs as follows.

6.1. Control Flow Attacks

Attacks associated with CF.BUSM. This CF (Figure 4) is susceptible to four attacks. (i) The *transmission* module GM.TX is susceptible to A7 (data injection into SSA repository) [47, 48], which exploits V2 (lack of authentication) [26]. GM.TX is also susceptible to A6 (denial of service), which exploits V2 in the module to gain unauthorized access to Starlink modems and modify the position of the antenna to prevent transmission/reception of RF signals (i.e., preventing the antenna on the ground and the antenna in the space from being in line of sight) [45]. (ii) The *command and data* module SM.C&DH is also susceptible to A9 (gaining control of satellites) [51], which also exploits V2 in the module to prevent the operating system from allocating resources to other bus system modules. (iii) The *electrical power* module SM.POWER, the *propulsion* module SM.PROP, and the *thermal control* module SM.THCTRL are susceptible to A8 (physical damage of satellites), which can be waged via electromagnetic pulses [49] or directed energy weapons [50].

Attacks associated with CF.REMM. This CF (Figure 5) is susceptible to A9 (gaining control of satellites), which exploits V2 (lack of authentication) in the *software access* module GM.SOFT to gain access to ground segment functions and control the space segment.

Attacks associated with CF.SUBSM. This CF (Figure 8) is susceptible to two attacks. (i) The *command and data* module SM.C&DH is susceptible to A9 (gaining control of satellites), which can execute a root-privileged bash script [46] or use a ransomware [51] to gain control of communications between the *communications payload* module (SM.PCOMMS) and the end user. (ii) The arc

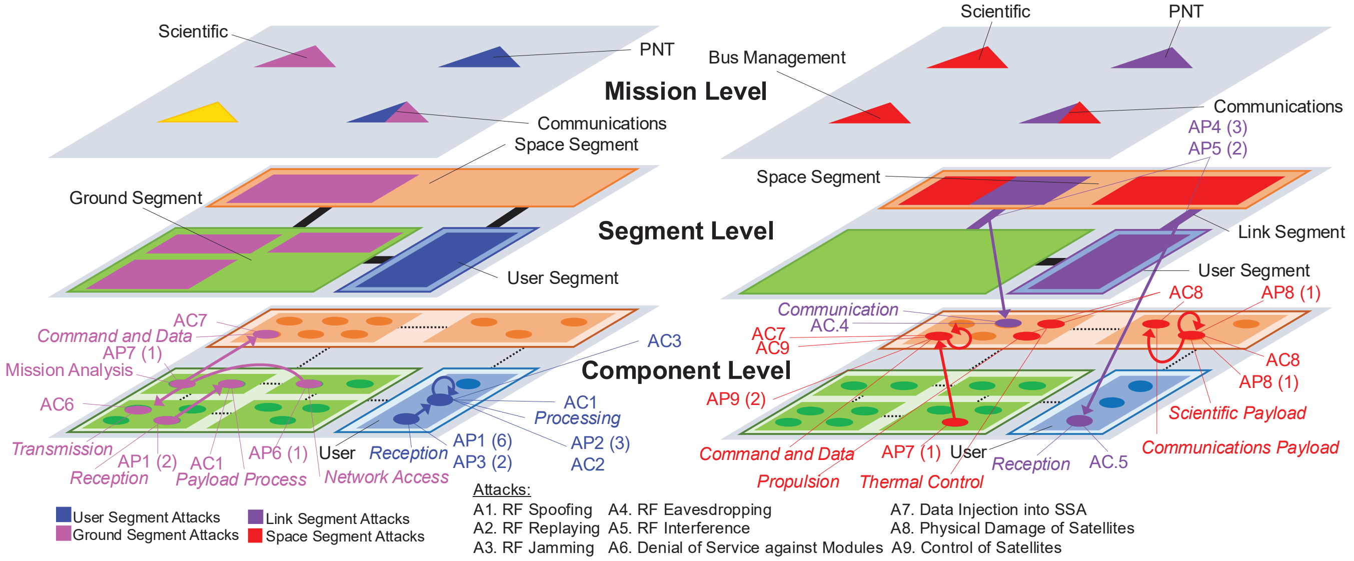

Figure 15: User, ground, link and space segment attacks studied in the literature and cast into the system model, where an attack is associated with one *attack point* (AP, which is the module serving as the entry point of the attacker into a space infrastructure) and a set of *attack consequence* points (ACs, which are the modules impacted by the attack, including AP). We use the following notation convention: "APx (y)" means y instance of attack Ax against module denoted by APx where $x \in \{1, \dots, 9\}$, and "ACx" means a module affected by Ax where AP$x \in \{\text{AC}x\}_x$. For instance, "AP1 (2)" means that there are two instances of A1 (spoofing attack) whose *attack point* is the *reception* module (AP1=GM.RX); and "AC1" means that the two instances of A1 have a consequence on the *payload process* module (AC1=GM.PAYPROC).

GM.TX→SM.COMMS (Figure 8) is inherently vulnerable to A4 (RF eavesdropping) against uplink transmissions [41].

Attacks associated with CF.TIMES. This CF (Figure 10) is susceptible to A6 (denial of service), which exploits V2 (lack of authentication) in the *transmission* module (GM.TX) to gain unauthorized access to Starlink modems and modify the position of the antenna to prevent transmission/reception of RF signals, namely preventing the antenna on the ground and the antenna in the space from being in line of sight [45].

Attacks associated with CF.SCI. This CF (Figure 12) is susceptible to A1 (RF spoofing), which exploits V2 (lack of authentication) in the *communications* module SM.COMMS to inject maligned scientific commands [23], causing the scientific payload to execute erroneous experiments.

6.2. Data Flow Attacks

Attacks associated with DF.TELEM. This DF (Figure 6) is susceptible to the following four attacks. The consequences of these attacks include stealing, manipulating, or denying operators from accessing, telemetry data. (i) The *command and data* module SM.C&DH is susceptible to A7 (data injection into SSA repository), which exploits V2 (lack of authentication) to enable the attacker to modify the heartbeat packets [22]. (ii) The SM.C&DH is also susceptible to A6 (denial of service), which exploits V2 in the module to inject resource-consuming bash scripts that execute as root, preventing the proper operation of the satellite [24, 46]. (iii) The *reception* module GM.RX is susceptible to A1 (RF spoofing), which exploits V2 in the module to spoof legitimate heartbeat packets [34, 35]. (iv) The arc SM.COMMS→GM.RX (Figure 6) is susceptible to A4 (RF eavesdropping), which exploits V3 (use of insecure protocol) [26] to intercept the communications between the two modules [52].

Attacks associated with DF.ORBM. This DF (Figure 7) is susceptible to two attacks. (i) The *analysis and support* module GM.A&S is susceptible to A9 (gaining control of satellites), which exploits V4 (incorrect EOL management) in the module to (e.g.) maneuver EOL satellites to endanger other satellites [28]. (ii) The *mission analysis* module GM.MA is susceptible to A7 (data injection into SSA repository), which exploits V2 (lack of authentication) in this module to manipulate the SSA repository [47, 48].

Attacks associated with DF.CHAO. This DF (Figure 9) is susceptible to the following three attacks, which can expose, degrade, or deny reception of, communications data. (i) The *reception* modules, UM.RX and GM.RX, are susceptible to A1 (RF spoofing), which exploits V2 (lack of authentication) in the modules to inject malicious data [25, 52]. (ii) The arcs SM.PCOMMS→UM.RX and SM.PCOMMS→GM.RX (Figure 9) are susceptible to A4 (RF eavesdropping), which exploit the inherent vulnerability of RF channels [52]. (iii) The same arcs are also inherently susceptible to A5 (RF interference) [43].

Attacks associated with DF.PNT. This DF (Figure 11) is susceptible to the following five attacks. (i) The *reception* module UM.RX is susceptible to A1 (RF spoofing), which exploits V2 in the module [29–32]. Note the ground segment *reception* module GM.RX should also be susceptible to A1; however, the literature has not studied this attack. (ii) The UM.RX is also susceptible to A3 (RF jamming), which is inherent [39]. Note that the ground segment *reception* module GM.RX is also susceptible to A3; however, the literature has not studied this attack. (iii) The *processing* module UM.PROC is susceptible to A2 (RF replaying), which is inherent [36, 37]. (iv) The arc SM.PNT→UM.RX (Figure 11) is susceptible to A4 (RF eavesdropping), which is inherent [40]. (v) The arc SM.PNT→UM.RX is also susceptible to A5 (RF interference) [40].

Attacks associated with DF.SCI. This DF (Figure 13) is susceptible to five attacks. (i) The *reception* module, GM.RX is susceptible to A1 (RF spoofing), which exploits V2 (lack of authentication) in the module [29–32]. (ii) The GM.RX is inherently susceptible to A3 (RF jamming)[39]. (iii) The *payload process* module GM.PAYPROC and the *processing* module UM.PROC are inherently susceptible to A2 (RF replaying) [38]. (iv) The arc SM.SCI→GM.RX (Figure 13) is inherently susceptible to A4 (RF eavesdropping) and A5 (RF interference) [40, 43].

Summarizing the preceding discussion, we draw:

Insight *2.* In the literature, the PNT broadcast data flow, DF.PNT, is most attacked, perhaps because it permits easy attacks that exploit either V2 (lack of authentication) or inherent vulnerabilities of RF signals.

7. Defenses

As highlighted in Figure 16, nine defenses have been reported in the literature: (D1) authenticating RF signals [53–67]; (D2) detecting spoofed RF signals [5, 68–95]; (D3) securing satellite management processes [28]; (D4) detecting and mitigating RF interference [42, 44, 95, 96]; (D5) mitigating RF eavesdropping [97–101]; (D6) detecting jamming [102, 103]; (D7) providing intrusion detection capabilities [46]; (D8) preventing radiation-induced bit errors [104]; (D9) applying traditional IT security mechanisms [105–108]. We map them to the CFs and DFs as follows.

7.1. Control Flow Defenses

Defenses associated with CF.BUSM. This CF (Figure 4) can be hardened by the following five defenses. (i) The *analysis and support* module GM.A&S can employ D3 (securing satellite management processes) to prevent attackers from exploiting V4 (incorrect satellite EOL management), by analyzing the location and state of EOL satellites to provide a deorbiting flight command and a payload management command to sanitize the payload modules in the satellite (e.g., powering off the *communications payload* module SM.PCOMMS to prevent an attacker from using the payload to jam the communications between other satellites) [28]. (ii) The *transmission* module GM.TX can employ D4 (detecting and mitigating RF interference) to mitigate A5 (RF interference), such as physical-layer countermeasures (e.g., manipulating physical-layer characteristics, such as adding artificial noise, and modifying the power allocation at the receiver end) [42]. (iii) The *communications* module SM.COMMS can also employ D4 to detect A5 [95, 96] and employ D6 (detecting jamming) to mitigate A3 (RF jamming) [102, 103]. (iv) The *command and data* module SM.C&DH can employ D7 (providing intrusion detection) to detect A6 (denial of service), A7 (data injection into SSA repository), and A9 (gain control of satellites) [46]. (v) The *electrical power* module SM.POWER, the *propulsion* module SM.PROP, the *thermal control* module SM.THCTRL, the *communications* module SM.COMMS, the *attitude control* module SM.ATCTRL, and the *command and data* module SM.C&DH can employ D8 (preventing radiation-induced bit errors) to mitigate A6 (denial of service), which leverages directed energy to induce bit errors [104].

Defenses associated with CF.REMM. This CF (Figure 5) can be hardened by employing D3 (securing satellite management processes) at the *analysis and support* module GM.A&S to protect V4 (incorrect satellite EOL management) [28] from being exploited.

Defenses associated with CF.SUBSM. This CF (Figure 8) can be hardened by the following two defenses. (i) The *transmission* modules, UM.TX and GM.TX, can employ D1 (authenticating RF signals) to mitigate A1 (RF spoofing) [63–66]. (ii) The *communications payload* module SM.PCOMMS can employ D4 (detecting and mitigating RF signal interference) [44, 95, 96] to prevent A5 (RF interference). SM.PCOMMS can also employ D6 (detecting jamming) to mitigate A3 (RF jamming) [102, 103].

Defenses associated with CF.TIMES. This CF (Figure 10) can be hardened by employing D1 (authenticating RF signals) at the *communications* module SM.COMMS to mitigate A1 (RF spoofing), where D1 can leverage either the physical characteristics of the signal received (e.g., signal and power distortion) [68–74], noise spatial correlation [75], Angle-of-Arrival [76], signal function [77–79], Direction-of-Arrival [80], carrier-phase measurements [81], signal correlation [82], and evaluating the time that takes the signal to traverse from the satellite to the receiver [83].

Defenses associated with CF.SCI. This CF (Figure 12) can be hardened by employing D4 (detecting and mitigating RF interference) at the *scientific payload* module SM.SCI [44, 95, 96] to mitigate A5 (RF interference). SM.SCI can also employ D6 (detecting jamming) [102, 103] to mitigate A3 (RF jamming).

7.2. Data Flow Defenses

Defenses associated with DF.TELEM. This DF (Figure 6) can be hardened by the following four defenses. (i) The *command and data* module SM.C&DH employs D7 (intrusion detection) to detect A6 (denial of service) and A9 (gaining control of satellites) [46]. (ii) The arc SM.COMMS→GM.RX (Figure 6) can be hardened by employing D5 (mitigating RF eavesdropping) [98] against A4 (RF eavesdropping), assuring the confidentiality of the telemetry data sent over the RF channel. (iii) The *reception*

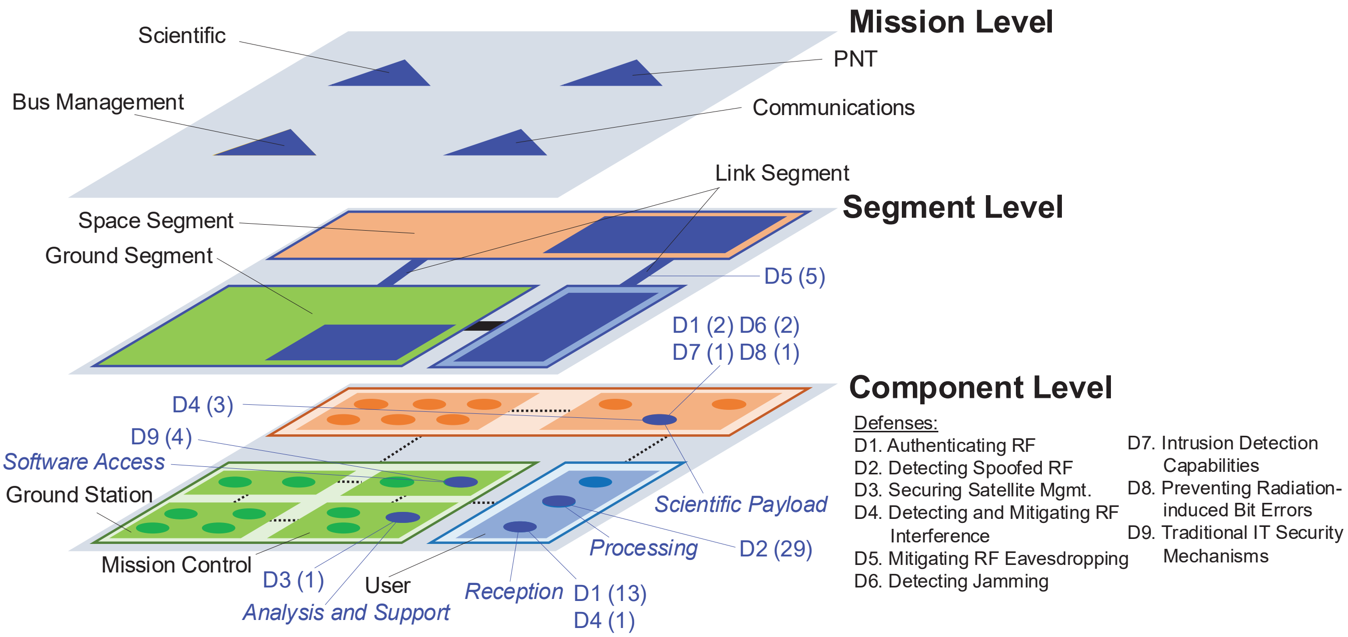

Figure 16: Defense mechanisms studied in the literature and cast in the system model, where "Da (b)" means b instances of defense Da can be employed at the module in question, where $a \in \{1, \ldots, 9\}$.

module GM.RX can employ D1 (authenticating RF signals) [53] to mitigate A1 (RF spoofing). (iv) The *telemetry* module GM.TELEM can be hardened by employing D9 (traditional IT security mechanisms) to mitigate A5 (RF interference), assuring the integrity of the telemetry data [106].

Defenses associated with DF.ORBM. This DF (Figure 7) can be hardened by two defenses. (i) The *analysis and support* module GM.A&S can use D3 (securing satellite management processes) [28] to mitigate A7 (data injection into SSA repository). (ii) The *mission analysis* module GM.MA can employ D9 (traditional IT security mechanisms) to mitigate A7, preventing attackers from gaining access to orbital data [107].

Defenses associated with DF.CHAO. This DF (Figure 9) can be hardened as follows. (i) The *transmission* module UM.TX can employ D1 (authenticating RF signals) to mitigate A1 (RF spoofing) and A2 (RF replaying), preventing a rogue communications satellite from receiving sensitive user data [63]. (ii) The *reception* modules, UM.RX and GM.RX, can employ D1 to mitigate A1 and A2, protecting communications data between users [54]. (iii) The arc SM.PCOMMS→UM.RX can employ D4 (detecting and mitigating RF interference) [42] and D5 (mitigating RF eavesdropping) [99] to mitigate A1, A2, A4 (RF eavesdropping), A5 (RF interference), and A6 (denial of service), assuring confidentiality and availability of user data.

Defenses associated with DF.PNT. This DF (Figure 11) can be hardened by five defenses. (i) The *PNT* module SM.PNT can employ D8 (preventing radiation-induced bit errors) to ensure the integrity of the PNT data that it produces. This is important because GNSS satellites orbit through the radiation-saturated Van Allen Belt [104], which could be exploited by attackers to camouflage their attacks in terms of the attack impact. (ii) The *reception* module UM.RX can employ D1 (authenticating RF signals) [77–79] and D6 (detecting jamming) [96] against A1 (RF spoofing), A2 (RF replaying), A3 (RF jamming), A5 (RF interference), and A6 (denial of service), assuring the availability and integrity of PNT data to users. (iii) The *mission analysis* module GM.MA can employ D1 (authenticating RF signals), such as GNSS receiver fingerprinting, to mitigate A1 (RF spoofing) and A2 (RF replaying), assuring the authenticity of the PNT data [61]. (iv) The *processing* module UM.PROC can employ D9 (traditional IT security mechanisms) to mitigate A1 (RF spoofing) and A2 (RF replaying), by increasing user awareness and recognition of false PNT data (e.g., a physical location derived from the PNT data substantially differs from inertial navigation system data) [108]. (v) The arc SM.PNT→UM.RX can employ D4 (detecting and mitigating RF interference) [42] and D5 (mitigating RF eavesdropping) [99] to mitigate A3 (RF jamming) and A4 (RF eavesdropping), assuring confidentiality of the PNT data and thus privacy of PNT users (i.e., their physical locations).

Defenses associated with DF.SCI. This DF (Figure 13) can be hardened by the following three defenses. (i) The *reception* module GM.RX can employ D2 (detecting spoofed RF signals) [77–79] and D6 (detecting jamming) [96] to mitigate A1 (RF spoofing) and A3 (RF jamming), assuring the detection of malicious RF signals. (ii) The *software access* module GM.SOFT can employ D9 (traditional IT security mechanisms) to mitigate A6 (denial of service) and A7 (data injection into SSA repository), protecting confidentiality, integrity and availability of the data processed in this module [105]. (iii) The arc SM.COMMS→GM.RX can employ D4 (detecting and mitigating RF interference) [42] and D5 (mitigating RF eavesdropping) [99] to mitigate A4 (RF eavesdropping) and A5 (RF interference), assuring confidentiality and availability of scientific data.

The preceding discussion leads to:

Insight ***3.*** Defending GNSS against spoofing attacks is most studied in the literature, and physical layer detection mechanisms (D2) are most popular.

As a caveat, Insight 3 pertains to academic literature. The popularity of GNSS defense in academic literature perhaps can be explained by Insight 2, namely that PNT broadcast data flow is most attacked in the literature.

8. Discussion

Connecting the "Dots." This corresponds to a meta analysis of Sections 5-7, which exhibits the bigger picture. Figure 17 maps mission CFs/DFs, vulnerabilities, attacks, and defenses systematized above. The usefulness of the mapping can be seen as follows. First, the mappings are largely many-to-many, indicating complexity of space cyber problems.

Second, by looking at the mission column and the mapping between it and the vulnerability column, we observe that CF.REMM, CF.SUBSM, and CF.TIMES have not been studied in security literature. We also observe how vulnerabilities are associated with the CFs and DFs, namely which CFs and DFs are impacted by which vulnerability. This paves a way for measuring the impact of a vulnerability when exploited, including the vulnerable and affected modules as per CVSS [109]. By looking at Figure 14, we observe the space segment has the most number of vulnerability instances (nine in total), while the ground and user segments have the least number of vulnerability instances (three in each case). However, this does not necessarily mean the ground or user segment is more secure than the space segment because, for instance, the former might be an easier target because (e.g.) the *ground station* component is often connected to the Internet as shown by CF.REMM).

Third, by looking at the vulnerability column and the mapping between it and the attack column, we observe that V2 (lack of authentication) is the most exploited vulnerability. By further looking at Figure 15, we observe: (i) an attacker can exploit two vulnerability instances of V3 (use of insecure protocol) in the ground segment to cause consequences to the space segment; (ii) the exploitation of 11 vulnerability instances in the space segment requires the attacker to have access to the ground segment; (iii) among the other vulnerability instances, only one instance can impact the space segment via the user segment (e.g., an attacker establishes a legitimate communication channel with the space segment by leveraging sensitive user channel subscription data). This paves a way for analyzing the likelihood that a vulnerability will be exploited, while leveraging subject matter expertise as in the current practice [110].

Fourth, by looking at the attack column and the mapping between it and the defense column, we observe: (i) which attacks can be mitigated by which defenses; (ii) there is a lack of studies on attacks that can physically damage satellites and defenses against them; (iii) there is one-to-one mappings between D2 (detecting spoofed RF signals) and A1 (RF spoofing), between D4 (detecting and mitigating RF interference) and A5 (RF interference), and between D5 (mitigating RF eavesdropping) and A4 (RF eavesdropping); (iv) D1 (authenticating RF signals) can mitigate A1 (RF spoofing), A2 (RF replaying), and A4 (RF eavesdropping); and (v) D6 (detecting jamming) can mitigate A3 (RF jamming) and A5 (RF interference).

Fifth, by looking at the defense column and leveraging the categorization of defenses in [111], we observe *preventive* and *reactive* defenses are most prominent in the literature, while *proactive* defenses are less investigated. By further looking at Figure 16, we observe that the user segment is the most investigated (43 defense instances in total), perhaps because it is less proprietary than the space or ground segment. These 43 instances belong to D1 (authenticating RF signals), D2 (detecting spoofed RF signals) and D4 (detecting and mitigating RF interference), meaning user segment defenses are mainly geared towards RF attacks.

The preceding discussion leads to:

Insight ***4.*** Attackers targeting the space segment have mainly pivoted through the ground segment; i.e., hardening the ground segment is an effective approach to protecting the space segment from cyber attacks.

Insight ***5.*** Current academic research mainly focuses on attacks and defenses of RF-related modules.

Future Research Directions. The preceding systematization leads to four research directions. The first direction is to investigate space infrastructures models. Our model is described at the *module* level of abstraction. How should the model be refined to a finer granularity and what is the optimal granularity?

The second direction is to refine the study on missions. We focus on some representative mission CFs and DFs. What is the complete, or as comprehensive as possible set of mission CFs and DFs? This is challenging because the classic textbook [16] on space engineering only provides a couple examples of something similar to our DFs, but lacks both technical details and consistent levels of abstraction. Another question is: How can we *completely* understand the interdependency between the components and/or modules in space infrastructures? For example, the *electrical power* module SM.POWER is not in the CF.SUBSM (subscription management) but can affect the latter because the *command and data* module SM.C&DH depends on SM.POWER to supply an appropriate voltage and sufficient amperage. Understanding these interdependencies is the first step towards taming space infrastructures resilience.

The third direction is to deepen our understanding of space infrastructure vulnerabilities and attacks. There are many open problems: What are the space-specific software and human vulnerabilities? What are the space-specific communications vulnerabilities? What are the space-specific supply chain vulnerabilities? What are the space-specific network-level, operating system-level, and application-level

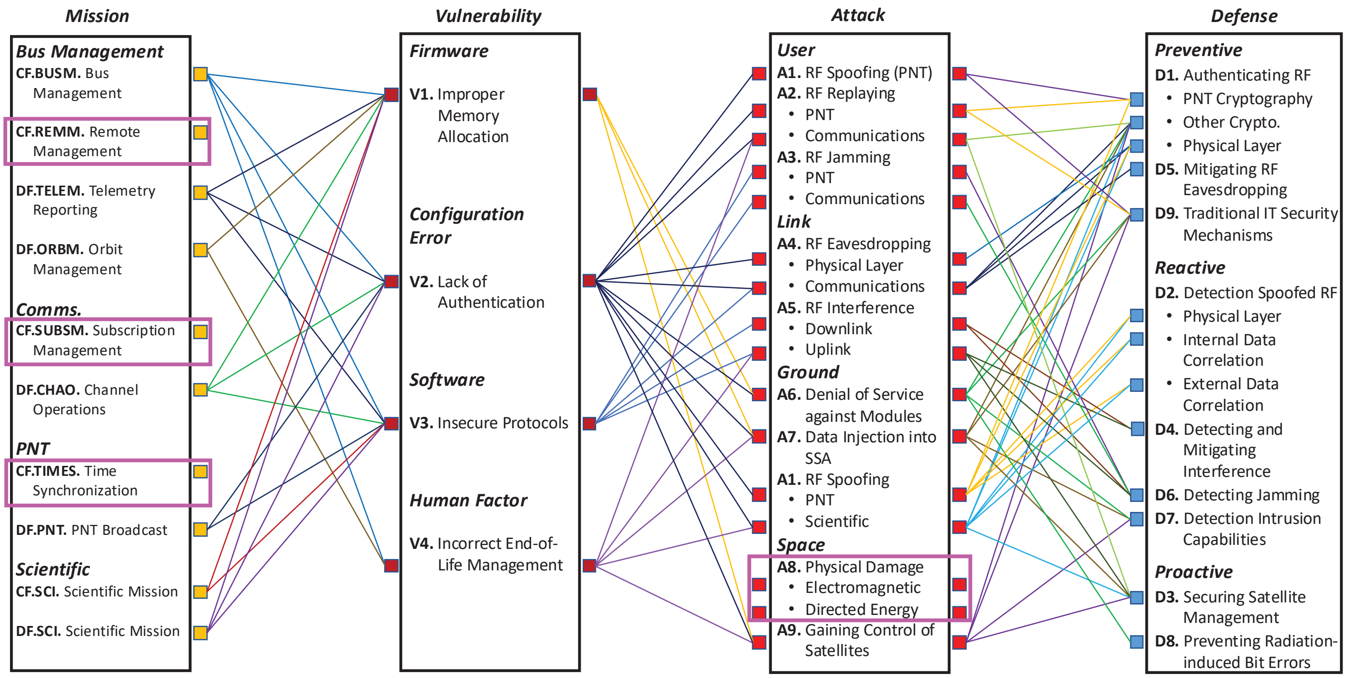
Mission
Bus Management
CF.BUSM. Bus Management
CF.REMM. Remote Management
DF.TELEM. Telemetry Reporting
DF.ORBM. Orbit Management
Comms.
CF.SUBSM. Subscription Management
DF.CHAO. Channel Operations
PNT
CF.TIMES. Time Synchronization
DF.PNT. PNT Broadcast
Scientific
CF.SCI. Scientific Mission
DF.SCI. Scientific Mission
Vulnerability
Firmware
V1. Improper Memory Allocation
Configuration Error
V2. Lack of Authentication
Software
V3. Insecure Protocols
Human Factor
V4. Incorrect End-of-Life Management
Attack
User
A1. RF Spoofing (PNT)
A2. RF Replaying
• PNT
• Communications
A3. RF Jamming
• PNT
• Communications
Link
A4. RF Eavesdropping
• Physical Layer
• Communications
A5. RF Interference
• Downlink
• Uplink
Ground
A6. Denial of Service against Modules
A7. Data Injection into SSA
A1. RF Spoofing
• PNT
• Scientific
Space
A8. Physical Damage
• Electromagnetic
• Directed Energy
A9. Gaining Control of Satellites
Defense
Preventive
D1. Authenticating RF
• PNT Cryptography
• Other Crypto.
• Physical Layer
D5. Mitigating RF Eavesdropping
D9. Traditional IT Security Mechanisms
Reactive
D2. Detection Spoofed RF
• Physical Layer
• Internal Data Correlation
• External Data Correlation
D4. Detecting and Mitigating Interference
D6. Detecting Jamming
D7. Detection Intrusion Capabilities
Proactive
D3. Securing Satellite Management
D8. Preventing Radiation-induced Bit Errors

Figure 17: Mapping of missions in terms of their CFs and DFs, vulnerabilities in terms of their classes, attack in terms of the segments they target, and defenses in terms of their nature, where pink boxes indicate topics that have not been studied in the security literature yet. The colors of the connections have no special meanings than helping distinguish between the lines (i.e., the lines associated with the same node on the left are in the same color).

attacks (e.g., remote code exploitation, API exploitation)? Which attacks exploiting space-specific management vulnerabilities do not have counterparts in the IT networks? What is the attack surface of satellite conjunction-prevention systems and how to minimize it? How should we measure the impact of vulnerabilities? As mentioned above, we propose to quantify it via their direct impact on the vulnerable module and cascading impact on other modules. In Figure 15, we made a conservative assumption about attack consequences because in principle, any module that is subsequent to the attack point (i.e., a module) in a CF/DF would be impacted. We plan to conduct experiments to validate this observation and measure the degrees of impacts.

The fourth direction is to investigate defenses. How should the user segment employ defenses to detect jamming attacks? How should we design ground segment defenses (e.g., input sanitization, access control, data execution prevention) to mitigate data injection and RF spoofing attacks? How should we design space segment defenses (e.g., real-time code analysis) to mitigate physical damage and satellite control attacks? How should we harden the existing or legacy space infrastructures and systems against cyber attacks? How can we make space infrastructures and systems resilient against cyber attacks? How can we make space-enabled communications resilient against jamming attacks? How can we leverage isolation to contain the impacts of attacks at the segment, component, and module levels?

Common to the four directions are three fundamental problems: defining metrics, building models, and experimental validation. In terms of defining metrics, there have been some substantial effort, including academic endeavors (e.g., [111–113]) and industrial endeavors (e.g., [109]). However, we anticipate a long journey to tackle this notoriously difficult problem. In terms of building quantitative space cyber risk models, there are early-stage endeavors (e.g.,[110, 114–117]). In terms of experimental validation of the theoretical models, there are initial proposals (e.g., [64, 118]).

9. Conclusion

We have presented a systematization of space infrastructures via five aspects: model, missions, vulnerabilities, attacks, and defenses. The systematization accommodates three levels of abstraction (i.e., mission vs. segment vs. component). Missions, infrastructure-level and application-level alike, are specified via their control flows and data flows, which serve as a basis for describing space infrastructures vulnerabilities, attacks, and defenses, as evidenced by the ones that are described in 87 literature studies. The systematization leads to a number of insights and future research directions, which hopefully will inspire more studies on the important topic of space cybersecurity.

Acknowledgments. We thank the anonymous reviewers for their constructive comments that helped improve the paper and our anonymous shepherd for reviewing our revised paper. This work is supported in part by the DoD UC2 program and NSF Grant #2308142. The opinions expressed

in the paper are that of the authors, and do not reflect the policy of any government agency in any sense.

References

[1] Space Foundation Editorial Team, "Space foundation releases the space report 2022 q2 showing growth of global space economy," https://www.spacefoundation.org/2022/07/27/the-space-report-2022-q2/.

[2] Space Foundation Editorial Team, "Space foundation releases the space report 2023 q2, showing growth of global space economy to $546b," https://www.spacefoundation.org/2023/07/25/the-space-report-2023-q2/.

[3] J. Pavur and I. Martinovic, "Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight," *Journal of Cybersecurity*, 2022.

[4] G. Falco and N. Boschetti, "A security risk taxonomy for commercial space missions," in *ASCEND 2021*, 2021, p. 4241.

[5] M. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Generalized likelihood ratio test for gnss spoofing detection in devices with imu," *IEEE TIFS*, 2021.

[6] E. Ear, J. L. Remy, A. Feffer, and S. Xu, "Characterizing cyber attacks against space systems with missing data: Framework and case study," in *2023 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2023, pp. 1–9.

[7] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the gnss spoofing threat and countermeasures," *ACM CSUR*, 2016.

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

[9] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE IoT-J*, 2019.

[10] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys & Tutorials*, 2021.

[11] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, 2022.

[12] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of gnss spoofing and anti-spoofing technology," *Remote Sensing*, 2022.

[13] M. Yuan, X. Tang, and G. Ou, "Authenticating gnss civilian signals: A survey," *Satellite Navigation*, 2023.

[14] X. Chen, R. Luo, T. Liu, H. Yuan, and H. Wu, "Satellite navigation signal authentication in gnss: A survey on technology evolution, status, and perspective for bds," *Remote Sensing*, 2023.

[15] D. Koisser, R. Mitev, N. Yadav, F. Vollmer, and A.-R. Sadeghi, "Orbital trust and privacy:{SoK} on {PKI} and location privacy challenges in space networks," in *33rd USENIX Security Symposium*, 2024.

[16] J. R. Wertz, D. F. Everett, and J. J. Puschell, *Space mission engineering: the new SMAD*. Microcosm Press, 2011.

[17] F. S. Prol, R. M. Ferre, Z. Saleem, P. Välisuo, C. Pinell, E.-S. Lohan, M. Elsanhoury, M. Elmusrati, S. Islam, K. Çelikbilek *et al.*, "Position, navigation, and timing (pnt) through low earth orbit (leo) satellites: A survey on current status, challenges, and opportunities," *IEEE Access*, 2022.

[18] S. Madry and S. Madry, "Applications of pnt systems," *Global Navigation Satellite Systems and Their Applications*, 2015.

[19] H. Li, X. Li, and J. Xiao, "Estimating gnss satellite clock error to provide a new final product and real-time services," *GPS Solutions*, 2024.

[20] C. R. Mercer, "Small satellite missions for planetary science," *33rd Annual AIAA/USU Conference on Small Satellites*, 2019.

[21] T. Scharnowski, F. Buchmann, S. Wörner, and T. Holz, "A case study on fuzzing satellite firmware," *Workshop on the Security of Space and Satellite Systems (SpaceSec)*, 2023.

[22] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *IEEE Symposium on Security and Privacy*, 2023.

[23] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "Sok: Security and privacy in the age of commercial drones," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021.

[24] B. Lin, W. Henry, and R. Dill, "Defending small satellites from malicious cybersecurity threats," in *ICCS*, 2022.

[25] D. Moser, P. Leu, V. Lenders, A. Ranganathan, F. Ricciato, and S. Capkun, "Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures," in *Proc. of ACM MobiCom*, 2016, pp. 375–386.

[26] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: on privacy and infrastructure security in dvb-s satellite broadband," in *Proceedings of ACM WiSec*, 2019, pp. 277–284.

[27] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky on the security of maritime vsat communications," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020.

[28] F. Lee and G. Falco, "The vulnerabilities less exploited: Cyberattacks on end-of-life satellites," EasyChair, Tech. Rep., 2023.

[29] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your gps are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX security symposium*, 2018, pp. 1527–1544.

[30] S. Islam, M. Z. H. Bhuiyan, I. Pääkkönen, M. Saajasto, M. Mäkelä, and S. Kaasalainen, "Impact analysis of spoofing on different-grade gnss receivers," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[31] S. Narain, A. Ranganathan, and G. Noubir, "Security of gps/ins based on-road location tracking systems," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 587–601.

[32] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of {Multi-Sensor} fusion based localization in {High-Level} autonomous driving under {GPS} spoofing," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 931–948.

[33] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, "An experimental study of gps spoofing and takeover attacks on uavs," in *31st USENIX Security Symposium*, 2022.

[34] E. Salkield, M. Szakály, J. Smailes, S. Köhler, S. Birnbach, M. Strohmeier, and I. Martinovic, "Satellite spoofing from a to z: On the requirements of satellite downlink overshadowing attacks," in *Proceedings of ACM WiSec*, 2023, pp. 341–352.

[35] E. Salkield, S. Birnbach, S. Kohler, R. Baker, M. Strohmeier, and I. Martinovic, "Firefly: spoofing earth observation satellite data through radio overshadowing," *Workshop on Security of Space and Satellite Systems (SpaceSec)*, 2023.

[36] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Location-independent gnss relay attacks: A lazy attacker's guide to bypassing navigation message authentication," *ACM WiSec 2023*, 2023.

[37] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Cryptography is not enough: Relay attacks on authenticated gnss signals," *arXiv preprint arXiv:2204.11641*, 2022.

[38] A. Costin, S. Khandker, H. Turtiainen, and T. Hämäläinen, "Cybersecurity of cospas-sarsat and epirb: threat and attacker models, exploits, future research," *arXiv preprint arXiv:2302.08361*, 2023.

[39] J. T. Curran, M. Bavaro, P. Closas, and M. Navarro, "On the threat of systematic jamming of gnss," in *ION GNSS+ 2016*, 2016.

[40] L. Crosara, F. Ardizzon, S. Tomasin, and N. Laurenti, "Performance evaluation of an indistinguishability based attack against spreading code secured gnss signals," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[41] D.-H. Jung, J.-G. Ryu, and J. Choi, "When satellites work as eavesdroppers," *IEEE Transactions on Information Forensics and Security*, 2022.

[42] L. Hu, S. Tan, H. Wen, J. Wu, J. Fan, S. Chen, and J. Tang, "Interference alignment for physical layer security in multi-user networks with passive eavesdroppers," *IEEE Transactions on Information Forensics and Security*, 2023.

[43] F. Rawlins, R. Baker, and I. Martinovic, "Death by a thousand cots: Disrupting satellite communications using low earth orbit constellations," *arXiv preprint arXiv:2204.13514*, 2022.

[44] G. Falco, N. G. Gordon, A. Byerly, A. Grotto, J. Siegel, and S. Zanlongo, "The space digital dome: Autonomous defense of space vehicles from radio frequency interference," in *2022 IEEE Aerospace Conference (AERO)*. IEEE, 2022, pp. 1–8.

[45] J. Smailes, E. Salkield, S. Birnbach, M. Strohmeier, and I. Martinovic, "Dishing out dos: How to disable and secure the starlink user terminal," *arXiv preprint arXiv:2303.00582*, 2023.

[46] J. P. Thebarge, W. Henry, and G. Falco, "Developing scenarios supporting space-based ids," in *ASCEND 2022*, 2022, p. 4219.

[47] J. Pavur and I. Martinovic, "On detecting deception in space situational awareness," in *Proceedings of ACM AsiaCCS*, 2021, pp. 280–291.

[48] J. Pavur and I. Martinovic, "The cyber-asat: on the impact of cyber weapons in outer space," in *2019 11th International CyCon*. IEEE, 2019.

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

[50] B. Cyr, Y. Long, T. Sugawara, and K. Fu, "Position paper: Space system threat models must account for satellite sensor spoofing," *SpaceSec23, Feb*, 2023.

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

[52] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity attacks on software logic and error handling within ads-b implementations: Systematic testing of resilience and countermeasures," *IEEE Transactions on Aerospace and Electronic Systems*, 2021.

[53] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil gps navigation message authentication," in *2014 IEEE/ION PLANS 2014*. IEEE, 2014.

[54] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-message robust authentication (chimera) for gps civilian signals," in *ION GNSS+ 2017*, 2017.

[55] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service," in *ION GNSS+ 2014*, 2014.

[56] I. Fernandez-Hernandez, J. Winkel, C. O'Driscoll, S. Cancela, R. Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, A. Dalla Chiara, C. Sarto, D. Blonski *et al.*, "Semi-assisted signal authentication for galileo: Proof of concept and results," *IEEE Transactions on Aerospace and Electronic Systems*, 2023.

[57] J. T. Curran and C. O'Driscoll, "Message authentica-

tion, channel coding & anti-spoofing," in *ION GNSS+ 2016*, 2016.

[58] Z. Wu, R. Liu, and H. Cao, "Ecdsa-based message authentication scheme for beidou-ii navigation satellite system," *IEEE Transactions on Aerospace and Electronic Systems*, 2018.

[59] R. X. Kor, P. A. Iannucci, L. Narula, and T. E. Humphreys, "A proposal for securing terrestrial radionavigation systems," in *ION GNSS+ 2020*, 2020.

[60] M. Arizabaleta, T. Pany, T. Scuccato, A. D. Chiara, C. O'Driscoll, and N. Hanley, "Receiver protocol and pitfalls of nma and sca processing under spoofing conditions for future gnss signals authentication," in *ION GNSS+ 2020*, 2020, pp. 3766–3780.

[61] D. Borio, C. Gioia, G. Baldini, and J. Fortuny, "Gnss receiver fingerprinting for security-enhanced applications," in *ION GNSS+ 2016*, 2016.

[62] Z. Zhu, S. Gunawardena, E. Vinande, and J. Pontious, "Identification of authentic gnss signals in time-differenced carrier phase measurements with a multi-constellation software defined radio receiver," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[63] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, "Qpep: An actionable approach to secure and performant broadband from geostationary orbit," in *Proc. of NDSS*, 2021.

[64] J. Huwyler, J. Pavur, G. Tresoldi, and M. Strohmeier, "Qpep in the real world: A testbed for secure satellite communication performance," in *Workshop on the Security of Space and Satellite Systems (SpaceSec)*, 2023.

[65] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "Anfra: Anonymous and fast roaming authentication for space information network," *IEEE TIFS*, 2019.

[66] G. Oligeri, S. Sciancalepore, S. Raponi, and R. D. Pietro, "Past-ai: Physical-layer authentication of satellite transmitters via deep learning," *IEEE TIFS*, 2023.

[67] C. Gudavalli, M. Goebel, T. Nanjundaswamy, L. Nataraj, S. Chandrasekaran, and B. S. Manjunath, "Resampling estimation based rpc metadata verification in satellite imagery," *IEEE TIFS*, 2023.

[68] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "Gnss signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, 2017.

[69] F. Rothmaier, L. Taleghani, Y.-H. Chen, S. Lo, E. Phelts, and T. Walter, "Gnss spoofing detection through metric combinations: Calibration and application of a general framework," in *Proceedings of ION GNSS+ 2021*, 2021.

[70] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, "A framework for gnss spoofing detection through combinations of metrics," *IEEE Transactions on Aerospace and Electronic Systems*, 2021.

[71] F. Rothmaier, Y.-H. Chen, S. Lo, J. Blanch, and T. Walter, "Providing continuity and integrity in the presence of gnss spoofing," in *ION GNSS+ 2021*, 2021.

[72] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for gnss-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, 2018.

[73] A. Rustamov, N. Gogoi, A. Minetto, and F. Dovis, "Gnss anti-spoofing defense based on cooperative positioning," in *ION GNSS+ 2020*, 2020.

[74] A. Jovanovic, C. Botteron, and P.-A. Fariné, "Multi-test detection and protection algorithm against spoofing attacks on gnss receivers," in *2014 IEEE/ION PLANS 2014*. IEEE, 2014.

[75] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver gps spoofing detection: Error models and realization," in *Proceedings of ACSAC*, 2016.

[76] S. Liu, X. Cheng, H. Yang, Y. Shu, X. Weng, P. Guo, K. C. Zeng, G. Wang, and Y. Yang, "Stars can tell: a robust method to defend against {GPS} spoofing attacks using off-the-shelf chipset," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021.

[77] E. Schmidt, N. Gatsis, and D. Akopian, "A gps spoofing detection and classification correlator-based technique using the lasso," *IEEE Transactions on Aerospace and Electronic Systems*, 2020.

[78] T. E. Humphreys, "Detection strategy for cryptographic gnss anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2013.

[79] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, 2013.

[80] S. Lo, Y. H. Chen, H. Jain, and P. Enge, "Robust gnss spoof detection using direction of arrival: Methods and practice," in *ION GNSS+ 2018*, 2018.

[81] E. Falletti, G. Falco, M. Nicola *et al.*, "Performance analysis of the dispersion of double differences algorithm to detect single-source gnss spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2021.

[82] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "Spree: A spoofing resistant gps receiver," in *Proceedings of ACM MobiCom*, 2016.

[83] Z. Chen, H. Li, Z. Ziheng, and M. Lu, "An approach to separate gnss spoofing signals from authentic signals using relative positioning," in *Proceedings of ION GNSS+ 2021*, 2021, pp. 3642–3652.

[84] W. Liu and P. Papadimitratos, "Probabilistic detection of gnss spoofing using opportunistic information," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[85] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Evaluation of the detection and mitigation of time synchronization attacks on the global positioning system," in *2018 IEEE/ION PLANS*. IEEE, 2018.

[86] J. Lee, E. Schmidt, N. Gatsis, and D. Akopian, "Anti-spoofing technique against gps time and position attacks based on sparse signal processing," in *Proceedings of ION GNSS+ 2021*, 2021, pp. 3581–3590.

[87] J. Smailes, S. Kohler, S. Birnbach, M. Strohmeier, and

I. Martinovic, "Watch this space: Securing satellite communication through resilient transmitter fingerprinting," *arXiv preprint arXiv:2305.06947*, 2023.

[88] M. Spanghero and P. Papadimitratos, "Detecting gnss misbehavior leveraging secure heterogeneous time sources," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[89] M. Spanghero and P. Papadimitratos, "High-precision hardware oscillators ensemble for gnss attack detection," in *2022 IEEE Aerospace Conference (AERO)*. IEEE, 2022, pp. 1–11.

[90] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks," in *2018 IEEE SP*. IEEE, 2018.

[91] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Exploiting side-information for resilient gnss positioning in mobile phones," in *2018 IEEE/ION PLANS*. IEEE, 2018.

[92] S. Baldoni, F. Battisti, M. Carli, and A. Neri, "A context-based framework for enhancing gnss performance and security," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[93] M. Spanghero, K. Zhang, and P. Papadimitratos, "Authenticated time for detecting gnss attacks," in *ION GNSS+ 2020*, 2020.

[94] K. Zhang, M. Spanghero, and P. Papadimitratos, "Protecting gnss-based services using time offset validation," in *2020 IEEE/ION PLANS*. IEEE, 2020.

[95] Z. Clements, T. E. Humphreys, and P. Ellis, "Dual-satellite geolocation of terrestrial gnss jammers from low earth orbit," in *2023 IEEE/ION PLANS*. IEEE, 2023.

[96] D. M. LaChapelle, L. Narula, and T. E. Humphreys, "Orbital war driving: Assessing transient gps interference from leo," in *ION GNSS+ 2021*, 2021.

[97] A. Vazquez-Castro and M. Hayashi, "Physical layer security for rf satellite channels in the finite-length regime," *IEEE TIFS*, 2019.

[98] M. G. Schraml, R. T. Schwarz, and A. Knopp, "Multiuser mimo concept for physical layer security in multibeam satellite systems," *IEEE Transactions on Information Forensics and Security*, 2021.

[99] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE TIFS*, 2015.

[100] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, and F. Gong, "Improving physical layer security of uplink noma via energy harvesting jammers," *IEEE Transactions on Information Forensics and Security*, 2021.

[101] M. Hayashi and A. Vazquez-Castro, "Physical layer security protocol for poisson channels for passive man-in-the-middle attack," *IEEE Transactions on Information Forensics and Security*, 2020.

[102] D. Borio, C. Gioia, A. Štern, F. Dimc, and G. Baldini, "Jammer localization: From crowdsourcing to synthetic detection," in *Proceedings of ION GNSS+ 2016*, 2016.

[103] J. Querol and A. Camps, "Real-time pre-correlation anti-jamming system for civilian gnss receivers," in *ION GNSS+ 2017*, 2017, pp. 1267–1288.

[104] M. Juliato and C. Gebotys, "A quantitative analysis of a novel seu-resistant sha-2 and hmac architecture for space missions security," *IEEE Transactions on Aerospace and Electronic Systems*, 2013.

[105] J. Pavur and I. Martinovic, "Sok: Building a launchpad for impactful satellite cyber-security research," *arXiv preprint arXiv:2010.10872*, 2020.

[106] C. Knez, T. Llansó, D. Pearson, T. Schonfeld, and K. Sotzen, "Lessons learned from applying cyber risk management and survivability concepts to a space mission," in *2016 IEEE Aerospace Conference*. IEEE, 2016.

[107] B. Young, "Commercial satellites, critical information infrastructure protection, and preventing today's threat actors from becoming tomorrow's captain midnight," *Strat Cyber Defense Multidisc Perspec*, 2017.

[108] T. Vera, "Cyber security awareness for smallsat ground networks," *30th Annual AIAA/USU Conference on Small Satellites*, 2016.

[109] Forum of Incident Response and Security Teams (FIRST), "Common Vulnerability Scoring System (CVSS)," https://www.first.org/cvss/.

[110] E. Ear, B. Bailey, and S. Xu, "Towards principled risk scores for space cyber risk management," *arXiv preprint 2402.02635*, 2024.

[111] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys (CSUR)*, 2016.

[112] J.-H. Cho, S. Xu, P. M. Hurley, M. Mackay, T. Benjamin, and M. Beaumont, "Stram: Measuring the trustworthiness of computer-based systems," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 128:1–128:47, 2019.

[113] S. Xu, "Sarr: A cybersecurity metrics and quantification framework," in *Third International Conference on Science of Cyber Security (SciSec'2021)*, 2021, pp. 3–17.

[114] S. Xu, "Cybersecurity dynamics," in *Proc. Symposium on the Science of Security (HotSoS'14)*, 2014, pp. 14:1–14:2.

[115] S. Xu, "Cybersecurity dynamics: A foundation for the science of cybersecurity," in *Proactive and Dynamic Network Defense*. Springer, 2019, vol. 74, pp. 1–31.

[116] S. Xu, "The cybersecurity dynamics way of thinking and landscape (invited paper)," in *ACM Workshop on Moving Target Defense*, 2020.

[117] Z. Lin, W. Lu, and S. Xu, "Unified preventive and reactive cyber defense dynamics is still globally convergent," *IEEE/ACM ToN*, vol. 27, no. 3, pp. 1098–1111, 2019.

[118] J. L. C. Remy, C. Chang, E. Ear, and S. Xu, "Space cybersecurity testbed: Fidelity framework, example implementation, and characterization," in *Proc. of SpaceSec*, 2025.

Appendix A. Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

A.1. Summary

This paper provides a systematization of space infrastructure cybersecurity. It introduces a threat taxonomy of attacks on satellite missions, the user, ground, and space segments, and the modules within each segment. The concepts of mission control flows and mission data flows are introduced to map vulnerabilities to specific operational functions based on an analysis of 87 prior works.

A.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field

A.3. Reasons for Acceptance

1) A well-executed methodology and systematization that provides a clear framework that simplifies the inherently complex space infrastructure environment.
2) Creates a new taxonomy for reasoning about satellite cybersecurity, which is a timely area to investigate given the rapid commercialization of the sector.

A.4. Noteworthy Concerns

1) The authors limit their discussion to primarily academic papers and do not provide a taxonomy of work that has occurred in industry, where a lot of the significant advances in space technologies are being made.
2) The paper focuses disproportionately on GNSS. While this has been a large area of academic research, the author should be careful to clarify and frame these findings as representing just one component of what could be many attack surfaces.
3) There is no discussion of how to quantify risk and vulnerability impact. The authors should discuss efforts that have been made to develop risk metrics in the space cybersecurity environment and describe which may be the most effective, particularly in the context of the taxonomy.

Appendix B. Response to the Meta-Review

- Response to Noteworthy Concern 1): We have conducted a systematic study on real-world cyber attacks against space infrastructures and systems [6], the outcome of which has been incorporated into the SPARTA space cyber attack database. Our ongoing research will likely lead to a substantially extended space cyber attack dataset, which will be incorporated into the SPARTA database as well.
- Response to Noteworthy Concern 2): In terms of the discussion on literature results, the disproportion is a natural reflection of the reality that GNSS is the most studied topic.
- Response to Noteworthy Concern 3): In the revised version, we have added a discussion on this topic. However, the status quo is that this topic is little understood, as evidenced by the fact that, to our knowledge, developing (most) effective risk metrics in space cybersecurity is an open problem and active research field. This can be evidenced by the fact that our research on quantitative space cyber risk management [110] has been incorporated into SPARTA version 1.6 in March 2024. Our ongoing research will lead to (at least) a new space cyber risk management framework, which is anticipated to be incorporated into the SPARTA standard as well.