Threat Modeling in Satellite Communications for Maritime Operations

Even Kvam Frøseth[1], Georgios Kavallieratos[1[0000−0003−1278−1943]], and Sokratis Katsikas[1[0000−0003−2966−9683]]

Department of Information Security and Communication Technology (IIK),
Norwegian University of Science and Technology, Gjøvik, Norway
evenkv@stud.ntnu.no, georgios.kavallieratos@ntnu.no,
sokratis.katsikas@ntnu.no

Abstract. The New Space Era and the emergence of high-bandwidth Low Earth Orbit (LEO) satellite constellations have caused a rapid change in the cyber threat landscape for industries reliant on satellite communications. One of these is the maritime sector. This work aims to analyze the threat landscape in satellite communications for maritime operations. To this end, an overview of the systems related to satellite communications in maritime operations is first provided. Then, three threat modelling methods, namely the STRIDE method, the Microsoft Threat Modelling Tool and the SPARTA framework are used to provide a holistic analysis of the threats in satellite communications at different, complementary levels. As an example, a sophisticated GPS spoofing attack that can cause major incidents for ships is analyzed in detail. The results will support the space sector towards improving the system architecture and making ship operations more secure.

Keywords: Space · Cybersecurity · Satellites · Threats · Maritime.

1 Introduction

Satellite communications are crucial for the global connectivity as they provide vital links to several industries such as maritime, energy, transportation and supply chain. The increased technological advancements of satellite technology, such as Low Earth Orbit (LEO) satellite constellations, expand the functions and operations of satellite communications. Such technological advancements brought significant opportunities but also came with significant security challenges. The term *New Space Era* describes the increased participation of private companies and commercial ventures in the space sector [12]. This has led to an explosion in the number of satellites in space today [1].

Satellite technology has historically relied on security through obscurity, assuming that limited access to technical details would protect against potential threats. Nowadays, the cybersecurity threats in space have increased and the

[1] Orbiting Now: https://orbit.ing-now.com

analysis of such threats and the identification of the appropriate controls are needed [2].

Nowadays, the maritime industry adopts low-latency, high-bandwidth, and cost-effective Internet through LEO satellite networks such as Starlink and OneWeb, to facilitate the core functions and operations. However, the integration of such technologies in the maritime industry increases the attack surface. A report with relevant cybersecurity incidents in the maritime sector illustrates the vulnerabilities and the threat landscape of the sector [14].

Maritime operations depend on satellite communications. The modern LEO satellite constellations pose a significant risk to the maritime sector and therefore the threat landscape and the potential cyber attacks should be analyzed. By leveraging a systematic analysis of the cyber threats posed by the space sector to the maritime sector, the most critical threats can be identified, analyzed, and mitigated.

This work explores the threats, vulnerabilities, and risks associated with integrating advanced satellite communication systems like Starlink into maritime operations. This is done by employing three distinct threat modeling methodologies, namely the STRIDE method, the Microsoft Threat Modeling Tool and the Space Attack Research and Tactic Analysis (SPARTA) framework. The STRIDE threat model provides a holistic view of the entire satellite communication system, from the ground stations and satellite constellation to a ship's satellite communication equipment and internal networks. The Microsoft Threat Modelling Tool supports the semi-automated implementation of STRIDE and provides threat analysis at a more detailed level than STRIDE itself. The SPARTA framework builds upon the MITRE ATT@CK framework and is used herein to facilitate the investigation of the Software-Defined Radio (SDR) for GPS spoofing to comprehensively analyze specific attack scenarios. The contributions of this work are as follows:

- Identifies the components of a state-of-the-art LEO satellite constellation.
- Analyzes the cybersecurity threats against LEO satellite components.
- Estimates the cyber risks of satellite communication in maritime operations.

The remainder of this article is structured as follows: Section 2 presents an overview of the satellite communication infrastructure. Section 3 reviews related work. In Section 4 we briefly discuss STRIDE, and the reasons that led us to use it, as well as the results of its application to the satellite communication infrastructure in maritime. In Section 5 the summary of the results is provided and finally, Section 6 summarizes our conclusions and proposes directions for future work.

2 Satellite Communications for Maritime Operations

Figure 1 provides a high-level overview of a system that uses a modern LEO satellite constellation for Internet through satellite communication. A large vessel is considered, since large ships highly rely on the Internet through satellite communication to operate. The assets of the space infrastructure are divided into four segments; these are the *space*, *link*, *ground*, and *user* segments [10].

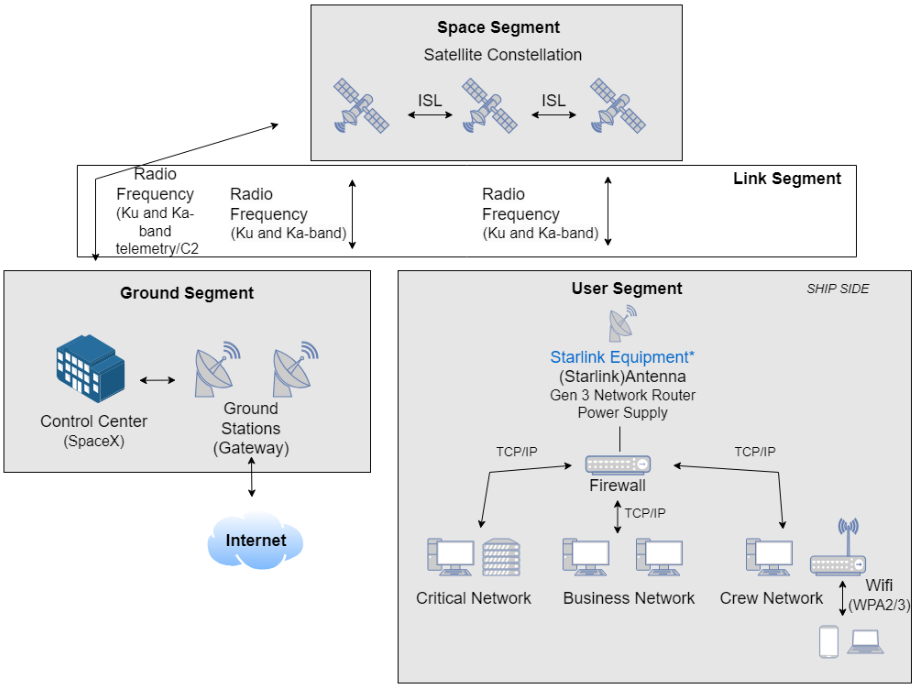


Fig. 1. Satellite Communication Overview.

The *space segment* entails all components designed to operate in space; this can include the following

The *link segment* provides the communication links to transmit data between the space segment to the ground and the user segments. This can be divided into *uplink*, *downlink*, and *crosslink*. The links can be [10]:

- Radio frequency (RF) communications link.
- Optical communication links. From ground to satellite and from satellite to satellite.

The *ground segment* contains all the terrestrial components and systems needed to properly operate, control, and support space-based assets. There is no publicly available information on Starlink's control centers. We can only assume that they operate as normal command centers, managing the constellation with telemetry and other data points. Ground stations are spread throughout the world to provide the maximum amount of coverage. The specifications of the ground stations are not publicly known, other than the modulation techniques and RF signal usage previously mentioned. Starlink uses a series of point-of-presence (POP) to connect to the internet backbone [24]. This can include [16, pp. 57–59]:

- Ground stations for uplink and downlink with antenna arrays and tracking systems.
- Control centers, including mission control, network operations centers, support infrastructure, and critical personnel for the operation of space-based assets.

The *user segment* entails all the elements that enable an end-user to access and utilize the data and services provided by space-based assets. The user segment is needed to transform the outputs from the space and ground segments to a usable application for the end user. The LEO user segment consists of the user terminal and other hardware and software [23]. This can include [10]:

- User equipment: antennas and satellite dishes, satellite phones and GPS receivers.
- Software applications like navigation and mapping.

The maritime domain is described within the user segment. The user segment consists of a firewall and three internal networks (*critical*, *business*, *crew*) on the ship. All the networks use generic standardized network protocols.

- Firewall: A generic firewall that sits between the Starlink user equipment and the three internal networks. The firewall monitors the network traffic and acts as a switch between the networks.
- Critical Network: The critical network contains network reliant systems that are deemed critical. These can include mail servers, database and storage solutions.
- Business Network: The business network contains all the network reliant systems used to conduct daily business on the ship. These can include desktop computers, laptops, and other relevant devices.
- Crew Network: The crew network consists of the crew wifi network solution and all devices connected to that network.

3 Related Work

A systematic literature review examines the cybersecurity aspects in space analyzing the space segment, the ground segment, and the user segment by leveraging the NIST cybersecurity framework, is provided in [10]. Threat modeling specifically focusing on satellites is a research area that has received significant attention. A comprehensive study on the challenges in threat modeling for new space systems is presented in [20]. STRIDE and DREAD are used to analyze the capability of existing threat modeling methods for capturing threats and security requirements from a system-centric approach. In [7], a threat model and security analysis of spacecraft computing systems is performed based on STRIDE and the critical assets in spacecraft systems are identified. In [18], a novel framework is presented that aims to assess the high-level resilience of the space systems considering specific types of threats. Willbold et al. [30] developed a taxonomy of threats against satellite firmware focusing on satellite-specific threat models. Pavur and Martinovic [17] provides a comprehensive analysis of the historical evolution and current state of cybersecurity threats targeting satellite systems. A comprehensive report on applying the NIST Cybersecurity Framework [2] to satellite command and control is presented in [13]. A conceptual model is proposed in [3] to study the space cybersecurity's challenges and opportunities emphasizing on the necessity of a comprehensive approach.

Kavallieratos et al. in [11] investigate cyberattacks against autonomous ships by leveraging the STRIDE methodology. A novel graphical security model named MV-HARM is proposed in [4] to analyze the security of maritime vessel networks. The cyber risks related to ship network infrastructure are discussed in [8]. The security of OPS-SAT CubeSat focusing on an attack targeting the mission's primary payload is provided in [1]. The cascading effects of cyberattacks against the space infrastructure are explored in [6], based on the complex network of interdependencies.

To the best of our knowledge, no previous work has implemented a holistic threat analysis to identify potential attacks against maritime operations that may occur in the space LEO infrastructure.

4 Threat Analysis in Satellite Communications for Maritime Operations

4.1 Methodology

STRIDE is a threat modeling methodology or framework originally created by Kohnfelder and Garg in 1999 and adopted by their employer Microsoft [3] in 2002 [21]. STRIDE is one of the most mature threat modeling frameworks and stands for the initials of the words *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service,* and *Elevation of Privilege* that correspond to the threat types that the method considers.

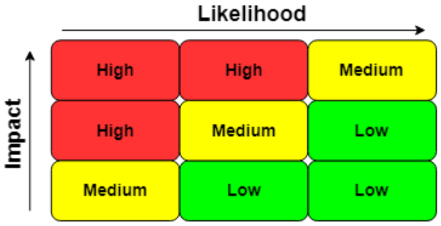
The STRIDE threat modeling process is usually divided into four steps [19]: *Step 1* consists of modeling a system in a diagram; the diagram type could be a data flow diagram (DFD), state lane diagram, swim lane diagram, or unified modeling diagram (UML). The most widely used diagram type is DFD [22, pp. 44]. *Step 2* consists of mapping the identified DFD elements to the STRIDE threat categories. A DFD element can be susceptible to more than one of the categories [19]. *Step 3* consists in extracting threats. Specific threats are extracted for each of the identified mappings between a DFD element and a threat

[2] NIST CSF: `https://www.nist.gov/cyberframework`

[3] Microsoft STRIDE: `https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN`

category. *Step 4* consists of documenting the identified threats in a structured format; this is often done using misuse cases [19].

It is important to note that we implemented STRIDE in the architecture depicted in Figure 1, considering the four space segments and their components. This allows us to extract results that remain valid despite internal architectural modifications, as long as each system or subsystem of the architecture remains operationally the same. The risk analysis is carried out by considering the likelihood of an attack and its impact. For the risk analysis we employed the risk matrix depicted in Figure 2 and used the criteria shown in Table 1 and in Table 2 to assess risk.



High	High	Medium
High	Medium	Low
Medium	Low	Low

Fig. 2. Risk matrix, based on [11].

Table 1. Impact criteria for satellite communication in maritime operations

Impact Criteria	
High (H)	1. Threats that may lead to the loss of human life. 2. Threats that may cause significant disruption to critical operations. 3. Threats that could result in major financial loss. 4. Threats that could result in unauthorized access to sensitive information. 5. Threats that could cause extensive service outage. 6. Threats that could compromise the integrity of command and control systems.
Medium (M)	1. Threats that could cause partial disruption of services. 2. Threats that may result in data manipulation. 3. Threats that could degrade communication quality 4. Threats that could result in unauthorized network access 5. Threat that could impact business operations. 6. Threats that may cause moderate economic impact.
Low (L)	1. Threats that could cause minor delays or disruptions. 2. Threats that may result in leakage of nonsensitive data. 3. Threats that could temporarily reduce service quality. 4. Threats that could cause brief communication interruptions. 5. Threats that could have minimal operational impact. 6. Threats that could lead to minor economic impact.

Table 2. Likelihood criteria for satellite communication in maritime operations

Likelihood Criteria	
Very Likely (VL)	1. The adversary is highly motivated and capable, with the skills and resources to exploit vulnerabilities, and there are no effective countermeasures deployed. 2. There are widely known and easily executable exploits targeting the system, which can be executed at any time by attackers. 3. The system, including satellite communications and ground stations, has high exposure to the internet and external networks, increasing the risk of attack. 4. There have been frequent past incidents indicating a high likelihood of similar attacks in the future.
Moderate (M)	1. The adversary is motivated and capable, but the system has some countermeasures that can mitigate the risk to a moderate level, but still be vulnerable. 2. The system has known vulnerabilities, but exploiting them requires physical access or specific conditions that are not always met. 3. Systems are indirectly exposed to the Internet or external networks, making it moderately challenging for attackers to reach and exploit them. 4. There have been occasional incidents or attempts indicating a moderate likelihood of similar attacks.
Rare (R)	1. The attacker is not highly motivated or lacks the necessary skills and resources to perform an attack, or the deployed countermeasures are highly effective. 2. An attacker must have administrative rights or specific, hard-to-obtain knowledge to perform the attack. 3. The system is not connected to external networks or systems, minimizing exposure. 4. There have been few to no past incidents, indicating a low likelihood of similar attacks occurring.

4.2 Applying STRIDE to Satellite Communications for Maritime Operations

A full analysis of threats against the Satellite Communication infrastructure as it is depicted in Figure 1 using STRIDE has been carried out. In the interest of adhering to space limitations, in this section we present a selected subset of the results of [5]. In the tables that follow ”I” stands for ”Impact”, ”L” stands for ”Likelihood” and ”R” stands for ”Risk”. Tables 3 to 10 show the threat analysis results.

Table 3. Control Center in STRIDE

	Control Center			
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof the identities of authorized personnel, gaining access to control center systems and issuing unauthorized commands to satellites.	H	M	H
T	An attacker could physically tamper with control center hardware, this can include servers, control terminals, and so on, ultimately installing malicious hardware or firmware, disrupting operations. An attacker could also tamper with the supply chain of hardware and/or software used in the control center to obtain the same results.	H	R	M
R	An attacker could manipulate control center access logs to obscure their actions, making it difficult to trace or prove malicious activities.	H	M	H
I	Sensitive operational information, such as satellite control commands or telemetry data, could be intercepted from the control center, leading to unauthorized access and data breaches.	H	M	H
D	An attacker could launch a DoS attack against control center systems, causing service outages and disrupting communications with the satellite constellation.	H	M	H
E	An attacker could exploit software vulnerabilities in control center systems to gain elevated privileges, allowing them to control or disrupt satellite operations.	H	R	M

Table 4. Ground stations in STRIDE

	Ground Stations			
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof the radio frequency signals used by the ground station to communicate with the satellites. This could lead to the ground station accepting false commands or telemetry data, disrupting satellite operations.	H	M	H
T	An attacker could physically tamper with the ground station's equipment, inserting malicious hardware or modifying existing components to disrupt communications or data integrity.	H	R	M
R	An attacker could perform actions within the ground station's network that go unlogged or mislogged, enabling them to deny responsibility for malicious activities and avoid detection.	M	M	M
I	Sensitive information, such as control commands and telemetry data, could be intercepted by an attacker during transmission between the ground station and satellites, leading to potential data breaches.	H	M	H
D	An attacker could launch a DDoS attack against the ground station, overwhelming its systems and causing a denial of service, disrupting communications between the station and the satellite network.	H	M	H
E	An attacker could exploit vulnerabilities within the ground station's software to gain elevated privileges, granting them unauthorized access to critical systems and the ability to issue commands to the satellites.	H	R	M

Table 3 shows the results of the STRIDE threat modeling in the Control Center. 4 high risks and 2 medium risks were identified. Table 4 shows the results of the STRIDE threat modeling on ground stations. 3 high risks and 3 medium risks were identified.

Table 5 shows the results of the STRIDE threat modeling on the LEO satellites. 3 high risks and 3 medium risks were identified. Table 6 shows the results of the STRIDE threat modeling on the Starlink equipment on board the ship. 4 high risks and 2 medium risks were identified.

Table 7 shows the results of the STRIDE threat modeling in the generic firewall between the Starlink user equipment and the 3 internal networks on board the ship. 3 high risks and 3 medium risks were identified. Table 8 shows the results of the STRIDE threat modeling in the critical network on the ship. 4 high risks and 2 medium risks were identified.

Table 9 shows the results of the STRIDE threat modeling in the business network on the ship. 1 high risk and 5 medium risks were identified. Table 10 shows the results of the STRIDE threat modeling in the crew network on the ship. 5 medium risks and 1 low risk were identified.

Table 5. LEO Satellites in STRIDE

LEO Satellites				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof the satellite communication signals, causing the satellites to accept false commands or telemetry data, potentially leading to incorrect positioning or data transmission errors.	H	M	H
T	An attacker could physically tamper with a satellite if they gain access to it, this could be done in orbit or by tampering with the satellite supply chain. The potential to insert malicious hardware, software, or modifying components is a possibility.	H	R	M
R	An attacker could manipulate logs or telemetry data to hide malicious activities, making it difficult to trace or prove their actions.	M	M	M
I	Sensitive information, such as encryption keys and satellite control data, could be intercepted by an attacker, leading to potential unauthorized access and data breaches.	H	M	H
D	An attacker could launch a jamming attack against the satellite's communication frequencies, causing a denial of service and disrupting communication with the ground stations or the ships Starlink equipment.	H	M	H
E	An attacker could exploit software vulnerabilities in satellite control systems to gain elevated privileges, allowing them to issue unauthorized commands and control the satellite.	H	R	M

Table 6. Starlink Equipment on ship in STRIDE

Starlink equipment on ship				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof the signals between the ship's antenna and the LEO satellites, causing the antenna to accept false commands or data, leading to incorrect operations or data corruption.	H	M	H
T	An attacker could physically tamper with the antenna or power supply on the ship, inserting malicious hardware or modifying components to disrupt communication or damage equipment.	H	M	H
R	An attacker could manipulate logs or records on the ship network, obscuring their actions and making it difficult to trace or prove malicious activities.	M	M	M
I	Sensitive information, such as encryption keys or operational data, could be intercepted from the ship antenna or network cables connected to equipment, leading to unauthorized access and data breaches.	H	M	H
D	An attacker could launch a jamming attack on the ship antenna, disrupting communication with the satellite and causing a denial of service.	H	M	H
E	An attacker could exploit vulnerabilities on the ship Starlink equipment software, gaining elevated privileges and unauthorized control over the communication system.	H	R	M

Table 7. Generic ship firewall in STRIDE

Generic ship firewall				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof the source IP address of a trusted network segment, for example the critical network, to bypass firewall rules and gain unauthorized access to sensitive systems and data.	H	M	H
T	An attacker could physically tamper with the firewall hardware, potentially inserting malicious components or modifying firmware to bypass security checks.	H	R	M
R	An attacker could compromise the firewalls logging and auditing mechanisms to alter logs, making it difficult to trace unauthorized activities and attribute malicious activities.	M	M	M
I	An attacker could exploit vulnerabilities in the firewall to intercept and access sensitive data being transmitted between the Starlink equipment and internal networks.	H	M	H
D	An attacker could overload the firewall with traffic (DDoS attack), causing it to fail and disrupting communications between the Starlink equipment and the internal networks.	H	M	H
E	An attacker could exploit software vulnerabilities in the firewall to gain elevated privileges, allowing them to modify rules and control network traffic.	H	R	M

Table 8. Critical network in STRIDE

Critical network				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof critical network credentials or communication protocols, gaining unauthorized access to critical systems and potentially causing critical disruptions or malicious activities.	H	M	H
T	An attacker could tamper with systems or devices with authorization in the critical network to insert malicious firmware or hardware, leading to disruptions or unauthorized access to data.	H	R	M
R	An attacker could manipulate logs or records within the critical network to obscure their actions, making it difficult to trace or prove malicious activities.	H	M	H
I	An attacker could gain unauthorized access to sensitive information on the critical network, such as navigation data, propulsion system controls, or critical safety system configurations.	H	M	H
D	An attacker could launch a DDoS attack against critical systems or devices on the critical network, causing a loss of availability and potentially disrupting critical ship operations.	H	M	H
E	An attacker could exploit a vulnerability in a critical system or device on the critical network, allowing them to gain elevated access and control over critical ship operations, including the ability to modify configuration settings and inject malware.	H	R	M

4.3 Microsoft Threat Modelling Tool

The Microsoft's Threat Modeling Tool (MTMT) allows the identification of potential threats which target data flows and back-end services of the system under analysis [9]. This tool allows the identification of security problems in processes, data stores and data flows, as the analysis is conducted using DFDs. Hence, DFDs for the satellite communication infrastructure for maritime operations are created.

MTMT comes with templates, and SDL TM Knowledge Base (Core)(4.1.0.11) was used as the base template for this analysis. The templates come with predetermined assumptions and descriptions and are usually related towards software-specific threat modeling. The main elements and parts of the template have been

Table 9. Business network in STRIDE

Business network				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof business network user credentials or communication protocols, gaining unauthorized access to sensitive business information and resources.	M	M	M
T	An attacker could tamper with devices like workstation and other devices connected to the business network, to insert malicious software or hardware, leading to data breaches and disruptions.	M	M	M
R	An attacker could manipulate business network logs to obscure their actions, making it difficult to trace or prove malicious activities.	M	M	M
I	Sensitive business information, such as financial data or intellectual property, could be intercepted from the business network, leading to data breaches and competitive disadvantages.	H	M	H
D	An attacker could launch a DoS attack against business network servers, causing service outages and disrupting business operations.	M	M	M
E	An attacker could exploit vulnerabilities in business network software or devices to gain elevated privileges, allowing them to access and manipulate sensitive data and systems.	H	R	M

Table 10. Crew network in STRIDE

Crew network				
T	**Threat description**	**I**	**L**	**R**
S	An attacker could spoof crew network credentials, gaining unauthorized access to personal information and potentially using the network as a pivot point to access other networks and systems onboard	M	M	M
T	An attacker could gain unauthorized access to a crew device or system on the crew network and modify its configuration or software, allowing them to disrupt or manipulate crew communications or steal personal data.	M	M	M
R	An attacker could manipulate logs or records on the crew network to obscure their actions, making it difficult to trace or prove malicious activities.	M	M	M
I	An attacker could gain unauthorized access to sensitive personal data from the crew on the crew network, such as identifiable personal information, financial data or medical records.	M	M	M
D	An attacker could launch a DDoS attack against crew devices or systems on the crew network, causing loss of availability and potentially disrupting the communication and morale of the crew. A DDoS attack could also lead to potential monetary loss to the crew, due to the limited data plan in maritime satellite Internet.	M	M	M
E	An attacker could exploit vulnerabilities in crew network software to gain elevated privileges, allowing them to access and manipulate personal data and network settings.	M	R	L

modified to represent the systems and components of the targeted infrastructure considering the Microsoft's user guide on MTMT [15]. The elements in the DFD are called *stencils* in MTMT. The definition of these five elements had to be adjusted in our STRIDE threat model. These are described in Table 11.

Table 11. MTMT element descriptions

Element	**Description**
Process	Represents a system component or operational entity involved in the satellite communication process.
External Interactor	Represents an external system or network interacting with the satellite communication system. For example, terrestrial internet backbone.
Data store	Any storage location for data, such as a database or file system.
Data flow	Represents the flow of data between system components or operational entities involved in the satellite communication process.
Trust Boundary	Boundary that defines areas of differing trust levels. Used to indicate where security controls are applied and where data transitions from one trust level to another.

The STRIDE threat modeling process is utilized by creating a DFD-diagram based on the identified assets of Section 2. The DFD-diagram is visualized in Figure 3. The threat model produced a total of 177 threats in the Satellite Communications infrastructure for Maritime Operations. MTMT has an export function that provides a report of the threats identified in the threat model.

In the interest of adhering to space limitations, in this section we present a selected subset of the results of [5]. Figure 4 shows an exported threat in the Denial of Service category, for the RF signal data flow between a ground station and a LEO satellite.

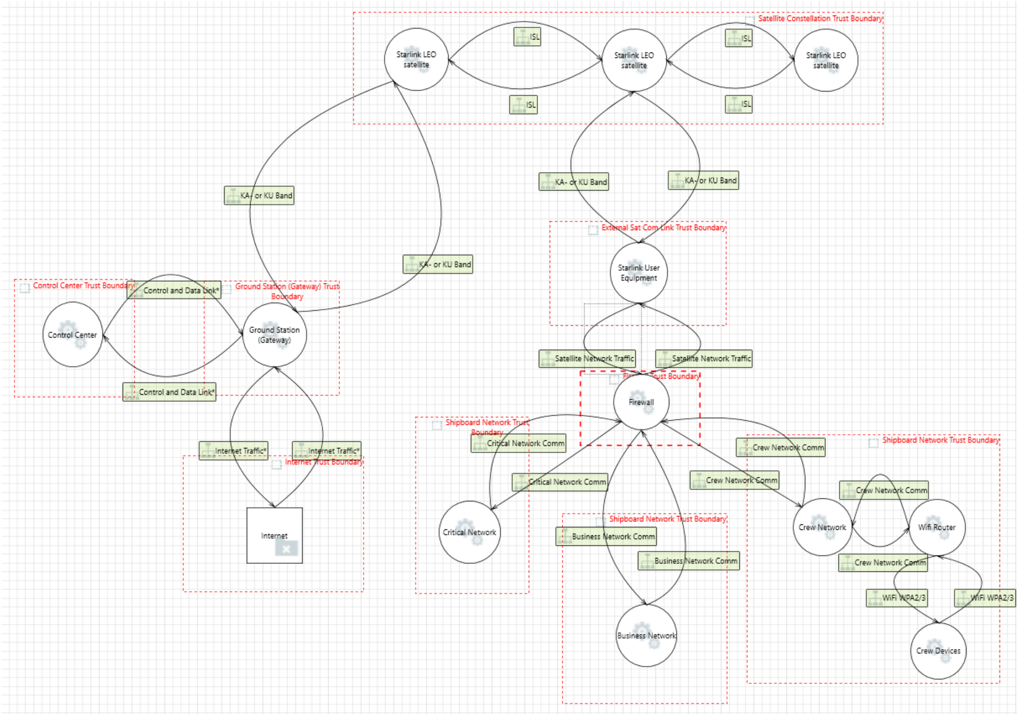
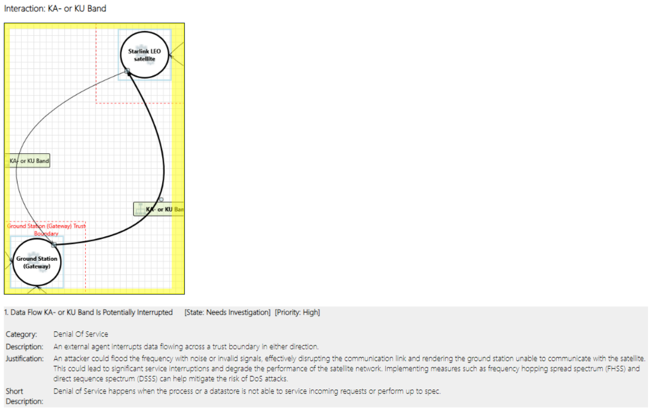


Fig. 3. Satellite Communications for Maritime Operations - DFD-diagram



1. Data Flow KA- or KU Band Is Potentially Interrupted [State: Needs Investigation] [Priority: High]

Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	An attacker could flood the frequency with noise or invalid signals, effectively disrupting the communication link and rendering the ground station unable to communicate with the satellite. This could lead to significant service interruptions and degrade the performance of the satellite network. Implementing measures such as frequency hopping spread spectrum (FHSS) and direct sequence spectrum (DSSS) can help mitigate the risk of DoS attacks.
Short Description:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.

Fig. 4. Interaction between Ka- or Ku-band for Ground Station and Satellite

4.4 SPARTA

In the previous analysis a holistic threat modeling approach was provided for the overall infrastructure. By focusing on particular critical assets identified from the STRIDE threat modeling, the Space Attack Research and Tactic Analysis (SPARTA) framework is applied. SPARTA is developed by The Aerospace Corporation to address the information and communication barrier in the space field [27]. SPARTA builds upon MITRE ATT&CK[4] and leverages unclassified research from academia and other credible information sources into cybersecurity matrices consisting of Tactics, Techniques, and Procedures (TPP). *Tactics* in SPARTA represent the tactical goals of the threat actor. These are: *Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Defense Evasion, Lateral Movement, Exfiltration, and Impact* [28]. *Techniques* are used to explain how a threat actor accomplishes a tactical objective through specific actions [29]. *Procedures* are used as a step-by-step description of the threat actors' use of tactics, techniques, and sub-techniques to achieve their initial tactical goal [26]. SPARTA also defines countermeasures that can be employed to prevent the successful execution of a technique or sub-technique. The countermeasures are made and mapped to standards such as NIST SP 800-53 [5] and ISO 27001 [6] [25]. The framework is not necessarily a traditional threat modeling framework, but can be utilized as an attack-centric threat modeling framework.

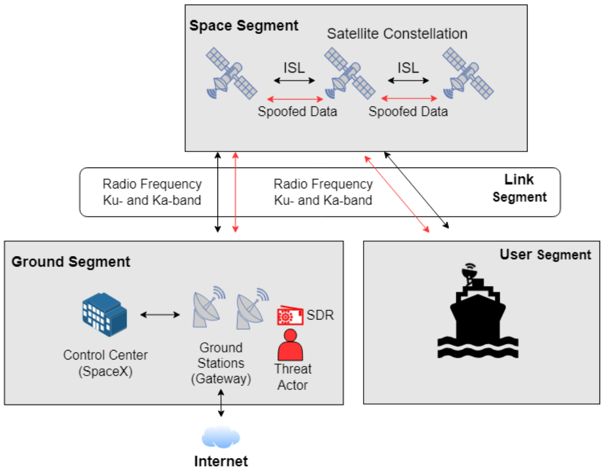


Fig. 5. Ground Station Spoofing Attack Through SDR.

In Figure 5 a threat actor compromises a ground station connected to the Starlink LEO satellite constellation and uses SDR to spoof GPS signals that are intended for a ship. SPARTA uses IDs to keep track of tactics, techniques, sub-techniques, and countermeasures. Figure 6 illustrates the applied SPARTA matrix.

[4] MITRE ATT&CK: https://attack.mitre.org/

[5] NIST SP 800-53: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[6] ISO 27001: https://www.iso.org/standard/27001

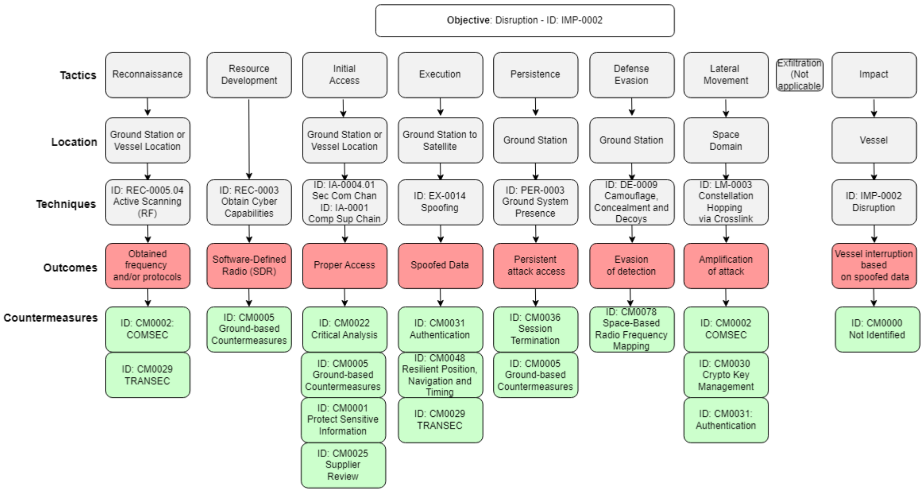

Objective: Disruption - ID: IMP-0002
Tactics
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Defense Evasion
Lateral Movement
Exfiltration (Not applicable
Impact
Location
Ground Station or Vessel Location
Ground Station or Vessel Location
Ground Station to Satellite
Ground Station
Ground Station
Space Domain
Vessel
Techniques
ID: REC-0005.04 Active Scanning (RF)
ID: REC-0003 Obtain Cyber Capabilities
ID: IA-0004.01 Sec Com Chan ID: IA-0001 Comp Sup Chain
ID: EX-0014 Spoofing
ID: PER-0003 Ground System Presence
ID: DE-0009 Camouflage, Concealment and Decoys
ID: LM-0003 Constellation Hopping via Crosslink
ID: IMP-0002 Disruption
Outcomes
Obtained frequency and/or protocols
Software-Defined Radio (SDR)
Proper Access
Spoofed Data
Persistent attack access
Evasion of detection
Amplification of attack
Vessel interruption based on spoofed data
Countermeasures
ID: CM0002: COMSEC
ID: CM0029 TRANSEC
ID: CM0005 Ground-based Countermeasures
ID: CM0022 Critical Analysis
ID: CM0005 Ground-based Countermeasures
ID: CM0001 Protect Sensitive Information
ID: CM0025 Supplier Review
ID: CM0031 Authentication
ID: CM0048 Resilient Position, Navigation and Timing
ID: CM0029 TRANSEC
ID: CM0036 Session Termination
ID: CM0005 Ground-based Countermeasures
ID: CM0078 Space-Based Radio Frequency Mapping
ID: CM0002 COMSEC
ID: CM0030 Crypto Key Management
ID: CM0031: Authentication
ID: CM0000 Not Identified

Fig. 6. Spoofing attack through SDR.

The SPARTA matrix consists of 9 tactics. *The Persistence* and *Evasive Action* tactics are combined in our threat model because they are relevant to the attack under analysis. Tactic *Exfiltration* is not considered, because it is not relevant to our scenario. An overview of the tactics with IDs is found in [28], techniques with IDs in [29], and countermeasures with IDs in [25].

The results of using SPARTA to analyze the specific attack follow.

Reconnaissance

- **Tactic ID:** ST0001
- **Tactic objective:** Obtain necessary information about the target ground station or vessel to facilitate further attacks.

The first step of the attack is the reconnaissance phase. The attacker aims to gather intelligence on the ground station or vessel connected to the Starlink LEO satellite constellation. The attacker takes the following steps to achieve the objective:

- **Technique ID:** REC-0005.04 - Active Scanning (RF)

The attacker uses a scanning device to identify and map the frequency and protocols used by the target ground station or vessel. The attacker also checks all available information sources that pertain to the details and security of the ground stations or the vessel.

ST0001 - Countermeasures To mitigate the risk associated with this reconnaissance tactic, the following countermeasures can be implemented:

- **CM ID:** CM0002 - Communications Security. Employ robust communications security measures to protect sensitive information transmitted over

communication channels. This includes secure communication protocols that utilize strong cryptographic mechanisms.
- **CM ID:** CM0029 - Transmission Security. Implement transmission security solutions to protect against RF scanning and eavesdropping. Jam-resistant waveforms, frequency hopping, and spread spectrum techniques can be used to obscure the communication signals.

Resource Development

- **Tactic ID:** ST0002
- **Tactic objective:** Develop or obtain the necessary resources and capabilities to support subsequent attack activities.

The attacker needs to acquire or develop tools, technologies, and capabilities required to execute the attack. This includes obtaining the necessary cyber capabilities to compromise the ground station and perform GPS spoofing. The following technique is used:

- **Technique ID:** REC-0003 - Obtain Cyber Capabilities. The attacker acquires or develops SDR technology and other cyber tools needed to spoof GPS signals.

ST0002 - Countermeasures Protection of terrestrial assets is in focus to protect from physical attacks on the ground station.

- **CM ID:** CM0005 - Ground-based Countermeasures Implement monitoring of suspicious activities and access control to prevent unauthorized access to ground stations. Intrusion detection systems can be used to identify potential threats.

Initial Access

- **Tactic ID:** ST0003
- **Tactic objective:** Gain unauthorized access to target.

In the initial access phase, the attacker aims to breach the security of the target ground station or vessel. Techniques used are:

- **Technique ID:** IA-0004.01 - Secondary/Backup Communication Channel
- **Technique ID:** IA-0001 - Compromise Supply Chain

The attacker could exploit vulnerabilities in secondary or backup communication channels to gain access to the ground station. This may involve targeting less secure backup systems or communication channels that are not as heavily monitored or protected. An attacker could also target the supply chain of components in the ground station, which includes both hardware and software. A supply chain compromise could give an attacker a backdoor into the ground station system.

ST0003 - Countermeasures Protecting against initial access to a system is a comprehensive task that requires a holistic view of the system to be able to mitigate threats.

- **CM ID:** CM0022 - Critical analysis. Critical analysis and risk assessment of critical components and the data flow of the ground station. This includes secondary and backup systems.
- **CM ID:** CM0001 - Protect Sensitive Information. Clear procedures on how to store and protect sensitive information should be implemented; this includes design and operational information for ground stations.
- **CM ID:** CM0025 - Supplier Review.
- A supplier review should be performed for all critical components of ground stations. This includes components and services of the ground station.

Execution

- **Tactic ID:** ST0004
- **Tactic objective:** Execute actions on the target to achieve intended malicious activity.

The execution phase implements the planned actions to manipulate or disrupt the target's operations. The primary objective in this use case is to spoof GPS signals that are intended for a vessel. The following technique is used:

- **Technique ID:** EX-0014 - Spoofing. The attacker uses the SDR technology from the resource development phase to generate and transmit false GPS signals. The spoofed GPS signals are specifically designed to deceive a vessel GPS receiver. Eventually, this leads to navigation errors, which could lead to operational disruptions or accidents.

ST0004 - Countermeasures Countermeasures that protect the RF signal from ground to satellite are important in the execution phase, the attacker has already established a foothold and has potentially acquired the necessary capabilities up until this phase.

- **CM ID:** CM0031 - Authentication. Robust authentication mechanisms for GPS signals should be implemented. This can include cryptographic authentication.
- **CM ID:** CM0048 - Resilient Position, Navigation and Timing. Resilient Positioning, Navigation, and Timing (PNT) solutions that can detect and mitigate the effect of GPS spoofing should be implemented. This can include multiple sources of PNT data and employing anti-spoofing and jamming mechanisms.

Persistence and Defense Evasion

- **Tactic ID:** ST0005
- **Tactic ID:** ST0006
- **Tactics objective:** Maintain a persistent presence, avoid detection, and evade defensive measures to maintain access and control over the target system.

The persistence and defense evasion phases are combined in our use case because they overlap to a large degree. In the persistence phase, the attacker focuses on establishing and maintaining a foothold within the target ground station. In the defense evasion phase, the attacker employs techniques to avoid detection by the target's security system and potential personnel. This is done to ensure the longevity of the attack and minimize the risk of being discovered and removed.

- **Technique ID:** PER-0003 - Ground System Presence
- **Technique ID:** DE-0009 - Camouflage, Concealment and Decoys

The attacker establishes persistent access within the ground station's systems or physical location. This can involve installing backdoors, maintaining control over compromised accounts, or leveraging existing vulnerabilities. It can also involve disguising physical access to the location of the ground station's location, eliminating physical security measures, including disabling monitoring and camera surveillance. This leads to the attacker having continuous access to the ground station.

ST0005 and ST0006 - Countermeasures An attacker who has persistent access to a system is problematic. It is hard to physically protect a ground station just because of the nature of how they have to operate; this includes the fact that they have to be spread around the world.

- **CM ID:** CM0036 - Session Termination. Strict session management and automatic termination of an inactive session should be implemented.
- **CM ID:** CM0078 - Space-based Radio Frequency Mapping. Space-based RF mapping should be implemented to detect anomalies in communication patterns.
- **CM ID:** CM0005 - Ground-based countermeasures. Comprehensive logging and monitoring systems to detect and analyze suspicious activities should be implemented.

Lateral Movement

- **Tactic ID:** ST0007
- **Tactic objective:** Move laterally within the target environment to access additional systems or data and expand the attack's impact.

In the lateral movement phase, the attacker seeks to exploit the Starlink satellite constellations crosslink capabilities to amplify the GPS spoofing attack.

- **Technique ID:** LM-0003 - Constellation Hopping via Crosslink. The attacker leverages inter-satellite links (ISLs) to hop from one satellite to another, with the potential of accessing different parts of the network or additional ground stations. This can amplify the attack to disrupt multiple vessels within a certain area relying on the same spoofed GPS data.

ST0007 - Countermeasures Potentially being able to move laterally in a compromised system is a major problem and can have a significant impact on the attack, by potentially amplifying spoofed data.

- **CM ID:** CM0002 - COMSEC. Encryption and secure communication protocols should be implemented to avoid compromise in the inter-satellite links.
- **CM ID:** CM0030 - Crypto Key Management. Best-practice cryptographic key management should be implemented to ensure that encryption keys are securely generated, distributed, and stored.
- **CM ID:** CM0031 Authentication. Strong authentication mechanisms should be implemented to verify entities that attempt to communicate or move laterally within the satellite constellation.

Impact

- **Tactic ID:** ST0009
- **Tactic objective:** Cause disruption to target vessel(s) through GPS spoofing.

The impact phase of the SPARTA matrix sets the ultimate goal for the attack.

- **Technique ID:** IMP-0002 - Disruption. The attacker uses the compromised ground station and spoofed GPS signals to mislead the vessel. This results in the vessel receiving incorrect navigation information, which can lead to operational disruptions, navigation errors, or physical accidents.

5 Summary of results and discussion

As already mentioned, 177 threats were identified during our STRIDE threat modeling in MTMT. This is consistent with the notion that STRIDE provides a large number of threats for complex systems and should be an iterative process throughout the lifetime of a system [21]. Threats identified through MTMT analysis are similar to the threats identified by the STRIDE methodology. However, the threats identified in the MTMT are more detailed, focusing on specific system/protocol vulnerabilities and complement the STRIDE analysis results. For example, the DoS threat in the ground station is described in STRIDE as *"An attacker could launch a DDoS attack against the ground station, overwhelming its systems and causing a denial of service, disrupting communications between the station and the satellite network"*. This same threat in the MTMT analysis is described in more detail: *"An attacker could flood the frequency with noise or invalid signals, effectively disrupting the communication link and rendering the ground station unable to communicate with the satellite. This could lead to significant service interruptions and degrade the performance of the satellite network. Implementing measures such as frequency hopping spread spectrum (FHSS) and direct sequence spectrum (DSSS) can help mitigate the risk of Dos attacks"*.

An overview of the results of the STRIDE threat model is provided in Table 12. The bottom row of the table shows a total risk score considering the criticality of each scenario (H=3, M=2, and L=1). This overview gives us a good understanding of the threats and risks throughout the system. Spoofing, Information Disclosure, and Denial of Service gathered the highest scores of cyber

Table 12. Overview of STRIDE threats and risks, based on [11]

STRIDE overview								
T	**Control Center**	**Ground Station**	**LEO Satellite**	**User Equipment**	**Ship Firewall**	**Critical Network**	**Business Network**	**Crew Network**
S	H	H	H	H	H	H	M	M
T	M	M	M	H	M	M	M	M
R	H	M	M	M	M	H	M	M
I	H	H	H	H	H	H	H	M
D	H	H	H	H	H	H	M	M
E	M	M	M	M	M	M	M	L
TR	**16**	**15**	**15**	**16**	**15**	**16**	**13**	**11**

risk. Tampering, Repudiation, and Elevation of Privilege are at a lower risk than the two aforementioned threats. This makes sense, particularly for Tampering and Elevation of Privilege, because they usually require a more sophisticated attack to materialize, compared to Spoofing, Information Disclosure, and Denial of Service.

The risks for each identified asset are high across the main maritime elements as these are described in Section 2. The Business Network and the Crew Network are identified as the assets with the lowest risk, with a total risk score of 13 and 11 respectively. The rest of the assets have a total risk score in the range of 15-16. This shows that proper management of the ship's network is an important factor in mitigating threats and risks in the user segment.

By leveraging an attack-centric approach, an attack that describes a GPS spoofing attack originating from a ground station, traveling through satellite communication to a target ship is analyzed. SPARTA is based on real-life information and data on space systems, which ensures that the threat model is grounded in reality and reflects the actual risks and vulnerabilities presented in satellite communication systems. The SPARTA matrix tooling also contributes to making the threat modeling process structured and comprehensive. SPARTA showed that a sophisticated GPS spoofing attack can be carried out to disrupt or potentially cause major incidents for ships. It also highlights the importance of securing ground stations, both physically and virtually.

Cybersecurity research in space infrastructure faces several significant limitations, which can impact the development and deployment of secure systems in this critical sector. Space systems operate in harsh environments, leading to unique technical challenges such as radiation effects, latency issues, and limited computational resources. These factors complicate the application of conventional cybersecurity measures. Furthermore, the lack of information regarding technical aspects of the space systems is among the main limitations when analyzing space infrastructure.

6 Conclusions

This work discussed the growing cyber threat landscape for maritime operations caused by the emergence of high-bandwidth, low-latency, and cost-efficient Internet through LEO satellite constellations. The components and cybersecurity threats of state-of-the-art LEO satellite constellations were presented. In addition, the threats and risks to satellite communication in maritime operations were identified. The threat analysis illustrated that LEO satellite constellations are complex systems that span multiple domains. STRIDE identified numerous threats and gave a holistic view of the threats to satellite communications by leveraging the MTMT analysis. Several observations were made through a risk assessment of the assets and threats identified. Spoofing, Information Disclosure, and Denial of Service had the highest risks in terms of threats. STRIDE and SPARTA were used to properly cover an under-researched area and give both a holistic and detailed view of threat modeling. As future work, we aim to further explore the threats against satellites used in the maritime sector by applying an automated tool and examine the propagation of the risks among critical infrastructures.

References

1. Calabrese, M., Kavallieratos, G., Falco, G.: A Hosted Payload Cyber Attack Against Satellites. In: AIAA SciTech Forum and Exposition, 2024. American Institute of Aeronautics and Astronautics Inc, AIAA (2024). https://doi.org/10.2514/6.2024-0270
2. Dark Reading Staff: Satellite Networks Worldwide at Risk of Possible Cyberattacks, FBI & CISA Warn (2022), https://www.darkreading.com/vulnerabilities-threats/satellite-networks-worldwide-at-risk-of-possible-cyberattacks-fbi-cisa-warn
3. Diro, A., Khan, S.K., Molla, A.: Leveraging system dynamic modelling for space cybersecurity conceptualisation and assessment. Available at SSRN 4671343
4. Enoch, S.Y., Lee, J.S., Kim, D.S.: Novel security models, metrics and security assessment for maritime vessel networks. Computer Networks **189** (4 2021). https://doi.org/10.1016/j.comnet.2021.107934
5. Frøseth, E.K.: Threat Modeling in Satellite Communications for Maritime Operations. Master's thesis, Norwegian University of Science and Technology (June 2024)
6. Hanan, J.T., Fowler, E., Hernandez, S., Niemczyk, M., Tatar, U., Keskin, O.F.: Analysis of satellite systems' dependencies and their cascading impacts. In: 2024 Systems and Information Engineering Design Symposium (SIEDS). pp. 493–498. IEEE (2024)
7. Hasan, R., Hasan, R.: Towards a Threat Model and Security Analysis of Spacecraft Computing Systems. In: 2022 IEEE International Conference on Wireless for Space and Extreme Environments, WiSEE 2022. pp. 87–92. Institute of Electrical and Electronics Engineers Inc. (2022). https://doi.org/10.1109/WiSEE49342.2022.9926912
8. Kaminska, N., Kravtsova, L., Kravtsov, H., Zaytseva, T.: Modeling ship cybersecurity using Markov chains: an educational approach. Tech. rep. (2024)

9. Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V., Wolthusen, S.: Threat analysis for smart homes. Future Internet **11**(10), 207 (2019)
10. Kavallieratos, G., Katsikas, S.: An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space. International Journal of Critical Infrastructure Protection **43** (12 2023). https://doi.org/10.1016/j.ijcip.2023.100640
11. Kavallieratos, G., Katsikas, S., Gkioulos, V.: Cyber-attacks against the autonomous ship. Tech. rep. (2019). https://doi.org/https://doi.org/10.1007/978-3-030-12786-2{_}2
12. Kodheli, O., Lagunas, E., Maturo, N., Sharma, S.K., Shankar, B., Montoya, J.F.M., Duncan, J.C.M., Spano, D., Chatzinotas, S., Kisseleff, S., Querol, J., Lei, L., Vu, T.X., Goussetis, G.: Satellite Communications in the New Space Era: A Survey and Future Challenges. IEEE Communications Surveys and Tutorials **23**(1), 70–109 (2 2020). https://doi.org/10.1109/COMST.2020.3028247, https://arxiv.org/abs/2002.08811v2
13. Lightman, S., Suloway, T., Brule, J.: NIST IR 8401 Satellite Ground Segment. Tech. rep. (2022). https://doi.org/https://doi.org/10.6028/NIST.IR.8401
14. Meland, P.H., Bernsmed, K., Wille, E., Rødseth, J., Nesheim, D.A.: A retrospective analysis of maritime cyber security incidents. TransNav **15**(3), 519–530 (2021). https://doi.org/10.12716/1001.15.03.04
15. Microsoft: Microsoft Threat Modeling Tool (2022), https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-feature-overview
16. Nejad, B.: Introduction to Satellite Ground Segment Systems Engineering (2023)
17. Pavur, J., Martinovic, I.: Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. Journal of Cybersecurity **8**(1) (2022). https://doi.org/10.1093/cybsec/tyac008
18. Plotnek, J., Slay, J.: A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems. Tech. rep. (2022), https://www.researchgate.net/publication/370102679
19. Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique. Requirements Engineering **20**(2), 163–180 (3 2015). https://doi.org/10.1007/s00766-013-0195-2
20. Sheik, A.T., Atmaca, U.I., Maple, C., Epiphaniou, G.: Challenges in threat modelling of new space systems: A teleoperation use-case. Advances in Space Research **70**(8), 2208–2226 (10 2022). https://doi.org/10.1016/j.asr.2022.07.013
21. Shevchenko, N., Chick, T.A., O'riordan, P., Scanlon, T.P., Woody, C.: Threat Modeling: A Summary of Available Methods (2018)
22. Shostack, A.: Threat Modeling: designing for security. Wiley, 1st edition edn. (2014)
23. Starlink: Flat High Performance Kit Specifications (2024), https://api.starlink.com/public-files/specification_sheet_flat_high_performance.pdf
24. Starlink: Starlink Point of Presence (2024), https://starlink-enterprise-guide.readme.io/docs/peering-with-starlink
25. The Aerospace Corporation: SPARTA Countermeasures (2022), https://sparta.aerospace.org/countermeasures/SPARTA
26. The Aerospace Corporation: SPARTA Procedures (2022), https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix
27. The Aerospace Corporation: SPARTA: Space Attack Research and Tactic Analysis (2022), https://sparta.aerospace.org/resources/getting-started

28. The Aerospace Corporation: SPARTA Tactics (2022), https://sparta.aerospace.org/tactic/SPARTA
29. The Aerospace Corporation: SPARTA Techniques (2022), https://sparta.aerospace.org/technique/SPARTA
30. Willbold, J., Schloegel, M., Vögele, M., Gerhardt, M., Holz, T., Abbasi, A.: Space Odyssey: An Experimental Software Security Analysis of Satellites (2023)