Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Even Kvam Frøseth

Threat Modeling in Satellite Communications for Maritime Operations

Master's thesis in Information Security
Supervisor: Sokratis Katsikas
Co-supervisor: Georgios Kavallieratos
June 2024

NTNU
Norwegian University of
Science and Technology

Even Kvam Frøseth

Threat Modeling in Satellite Communications for Maritime Operations

Master's thesis in Information Security
Supervisor: Sokratis Katsikas
Co-supervisor: Georgios Kavallieratos
June 2024

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Threat Modeling in Satellite Communications for Maritime Operations

Even Kvam Frøseth

10.06.2024

Acknowledgments

First of all, I would like to thank my supervisors Georgios Kavallieratos and Sokratis Katsikas for their invaluable support and feedback throughout this process. Their previous research has been fundamental for the development of this thesis. Friends and family have been instrumental in these master studies. Lastly, I would like to thank Hilde Bakke, from the Faculty of Information Technology and Electrical Engineering for her continuous support.

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. The maritime sector has been dependent on satellite communications for decades and is one of the industries most affected by this massive change in Internet connectivity through satellite communication.

This master thesis aims to provide insight into this growing threat landscape by identifying components and cybersecurity threats towards state-of-the-art LEO satellite constellations, investigating threat modeling frameworks and their applicability to threat modeling for satellite communications in maritime operations, and identifying threats and risk for satellite communication in maritime operations.

This is done through a qualitative approach and utilizes threat modeling in two use cases relevant to satellite communication and maritime operations. STRIDE and SPARTA matrix were applied to these use cases and found 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. SPARTA showed that a sophisticated GPS spoofing attack can be carried out to disrupt or potentially cause major incidents for ships.

Sammendrag

Den nye romalderen og fremveksten av høy båndbredde Low Earth Orbit (LEO) satellittkonstellasjoner har forårsaket en raks endring i trussel landskapet for cybertrusler i industrier som er avhengige av satellittkommunikasjon. Sjøfartssektoren har vært avhengig av satellittkommunikasjon i flere tiår og er en av de industriene som er mest påvirket av denne massive endringen i Internett-tilkobling gjennom satellittkommunikasjon.

Denne masteroppgaven har som mål å gi innsikt i dette voksende trussel landskapet ved å identifisere komponenter og cybersikkerhetstrusler mot toppmoderne LEO satellittkonstellasjoner, undersøke trussel modellering rammeverk og deres anvendbarhet for trussel modellering for satellittkommunikasjon i maritime operasjoner, og identifisere trusler og risiko for satellittkommunikasjon i maritime operasjoner.

Dette gjøres gjennom en kvalitativ tilnærming og benytter trussel modellering i to brukstilfeller som er relevante for satellittkommunikasjon og maritime operasjoner. STRIDE og SPARTA-matrisen ble anvendt på disse brukstilfellene og fant at LEO satellittkonstellasjoner er komplekse systemer som spenner over flere domener. STRIDE identifiserte mange trusler og ga en helhetlig oversikt over truslene mot satellittkommunikasjon. SPARTA viste at et sofistikert GPS-spoofing angrep kan utføres for å forstyrre eller mulig forårsake store hendelser for skip.

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Justification and Motivation

Satellite communications have played an important role in global connectivity for years, offering vital links to various industries, including the maritime sector. Satellite technology has historically relied on security through obscurity, assuming that limited access to technical details would protect against potential threats. However, the rapid evolution of satellite technology, particularly with the advent of Low Earth Orbit (LEO) satellite constellations, has dramatically expanded the capabilities and reach of satellite communications. This technological advancement has brought significant opportunities, but also comes with significant challenges.

The term *New Space Era* refers to a shift in the space industry from being dominated by government agencies to an increased participation by private companies and commercial ventures [1]. This has led to an explosion in the number of satellites in space today. A satellite tracking website [1] estimates that a total of 10060 satellites are orbiting the Earth today. The threat landscape in space has grown dramatically because of this, and in 2022 we saw the FBI and CISA ring the alarms about possible threats to satellite communication systems and urged satellite communication providers to take immediate mitigation steps, including deploying encryption, hardening authentication, and patching software [2].

The maritime industry has historically been plagued with slow and expensive internet through satellite communications, but that is changing with the low-latency, high-bandwidth, and cost-effective Internet through LEO satellite networks like Starlink and OneWeb, this also makes the maritime industry more susceptible to cyber incidents. A 2021 study analyzed 46 maritime cyber security incidents in the last decade and found that the sector has a low frequency but high impact in terms of incidents, with a growing trend of cyber-exposed systems [3].

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

1.2 Planned Contributions

The goal of this thesis is to shed light on an ever-growing problem that is not receiving the attention it needs. Maritime operations are dependent on satellite communications and the increased threat landscape caused by modern LEO satellite constellations needs to be investigated.

This thesis aims to explore the threats, vulnerabilities, and risks associated with integrating advanced satellite communication systems like Starlink into maritime operations. This is done by employing two distinct threat modeling methodologies, STRIDE and the Space Attack Research and Tactic Analysis (SPARTA) framework.

The STRIDE threat model offers 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. This model identifies threats related to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege across the various identified components and trust boundaries within the system.

The thesis also leverages the SPARTA framework to investigate the use of Software-Defined Radio (SDR) for GPS spoofing to get a deeper understanding of specific attack scenarios. This scenario examines how an attacker could exploit ground stations to transmit false GPS signals through the satellite constellation to a target ship. It also looks into the possibility of using LEO satellite constellations to amplify attacks.

1.3 Keywords

Satellite communication, maritime operations, LEO satellite constellations, threat modeling, cybersecurity, threat, risk

1.4 Research Questions

The following research questions have been developed based on Sections 1.1 and 1.2

- RQ 1: Cybersecurity in Low Earth Orbit (LEO) Satellite Constellations
  - RQ 1.1: What are the components of a state-of-the-art LEO satellite constellation?
  - RQ 1.2: What are the cybersecurity threats against LEO satellite components?
- RQ 2: What are the most prevalent threat modeling frameworks and what frameworks are best suited for threat modeling for satellite communications in maritime operations?

- RQ 3: What are the identified threats and risks to satellite communication in maritime operations?

1.5 Thesis Structure

The thesis is structured as follows:

- **Chapter 2:** Gives a comprehensive view of relevant background information, including satellite communications systems and threat modeling frameworks.
- **Chapter 3:** reviews existing literature related to threat modeling in satellite communications and maritime operations.
- **Chapter 4:** outlines the thesis research design and justifies the methodological choices made to answer the research questions presented in chapter 1.
- **Chapter 5:** presents the results from the threat modeling process done on our use cases.
- **Chapter 6:** discusses the results of the thesis in relation to the research questions. It also elaborates on the limitations of the research project.
- **Chapter 7:** concludes the research project and provides suggestions for future work.

Chapter 2

Background

This chapter starts of by giving a comprehensive overview of satellite communication systems and key aspects such as networking protocols and radio frequency signals. It also highlights cybersecurity challenges and the emergence of LEO satellite constellation. Finally, it introduces a range of threat modeling frameworks and put them into context.

2.1 Overview of Satellite Communication Systems

Satellite communication systems rely on space infrastructure to operate. The space infrastructure is the backbone of all activities that involve space in any capacity. [4] divides space in to four distinct segments. Space, link, ground, and user segments.

The space segment entails all components designed to operate in space, this can include the following [5, p. 33].

- Communication satellites, navigation satellites, scientific satellites and more.
- Other spacecrafts including probes, space stations, and telescopes.

The link segment is the communication pathways needed 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 [4]:

- 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. This can include [5, 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. This can include [4]:

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

Satellite types are usually divided into categories on the basis of where it operates in orbit in relation to Earth and what purpose it is supposed to serve. These categories are Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geo-stationary Earth Orbit (GEO) and Highly Elliptical Orbit (HEO) [6].

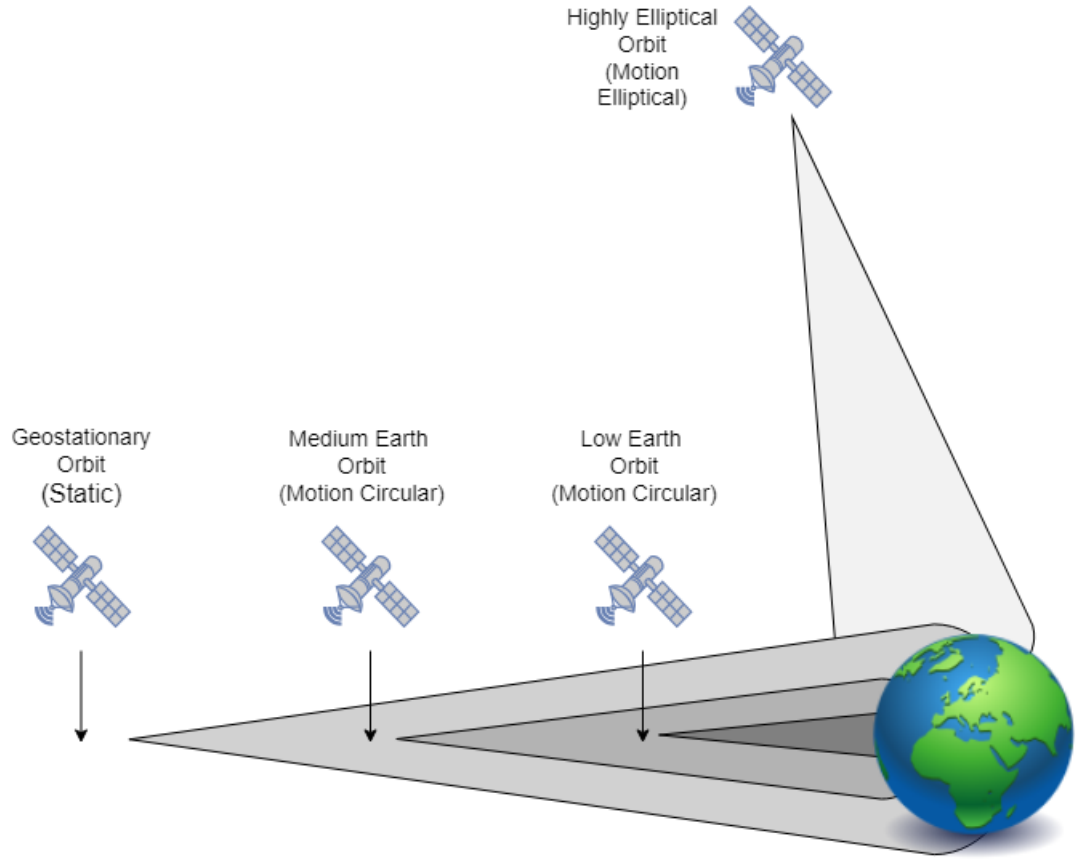


Figure 2.1: LEO, MEO, GEO, HEO satellites visualized

Based on the orbit in which the satellites operate we get different characteristics and use cases.

2.1.1 Low Earth Orbit (LEO) Satellites

LEO satellites operate in a circular orbit at an altitude ranging from 180 to 2000 km above the Earth's surface. The orbital period ranges from 90 to 120 minutes, depending on the altitude. The satellites can be deployed in an elliptical orbit, but this is not common for the majority LEO satellites in orbit today [7] [8].

The low latency and high data transmission speed are made possible because of their low altitude. This makes LEO satellites a true alternative for real-time applications such as high-bandwidth and availability for internet services to industries that rely on satellite internet. The low latency and high data transmission is only improving due to the emergence of LEO satellite constellations [9]. LEO satellites are subject to more atmospheric drag than satellites in other orbital categories, leading to faster orbital decay, resulting in frequent adjustments and replacements [10].

2.1.2 Medium Earth Orbit (MEO) Satellites

MEO satellites generally operate in a circular orbit at an altitude ranging from 8000 to 20000 km above the Earth's surface. The orbital period ranges from 6 to 14 hours [7]. MEO satellites have much better coverage than LEO satellites and rely on less frequent handovers at the cost of signal propagation delay or latency. Global navigation satellite systems such as the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS), and Compass Navigation Satellite System (CNSS) prefer MEO over LEO and GEO because of the middle ground it provides when it comes to global coverage and latency. A total of 31 MEO satellites are needed for GPS to have global coverage [11].

2.1.3 Geo-stationary Earth Orbit (GEO) Satellites

GEO satellites operate in a circular orbit at an altitude of 35786 km above the Earth's surface. GEO satellites appear to be static because the satellite is in Earth's equatorial plane and the orbital period is 24 hours, which means that the satellite is matching Earth's rotation [7]. A single GEO satellite can provide coverage over approximately one third of the Earth's surface and is primarily used for satellite TV and operations reliant on continuous coverage. Terrestrial antennas can be fixed because the satellite appears stationary. This comes at the cost of latency and bandwidth capabilities [12].

2.1.4 Highly Elliptical Orbit (HEO) Satellites

HEO satellites operate in an elliptical orbit with varying altitudes. It has a perigee of about 500 km above the Earth's surface and an apogee of around 50000 km [13]. The elliptical orbit allows a HEO satellite to spend extended periods of time over specific areas. A two HEO satellite system will be able to provide continuous coverage over a region, this is often done in the polar regions [14].

2.2 Satellite Communication

A variety of technologies, including networking protocols and techniques, must work in unison to make satellite communication a reality. A generic satellite communication has to involve certain steps [15, pp. 28–30].

Uplink: The transmission starts at the ground station, data being sent is converted into radio frequency (RF) signal through a process called modulation. The RF signal is amplified and passed through the ground stations antennas.

Satellite reception: A transponder on the satellite receives the RF signal, shifts the RF signal to a different frequency band and amplifies the RF signal in preparation to send back to a ground station.

Downlink and ground station processing: Satellite takes the processed RF signal and sends it back to an ground station through its downlink antennas. Ground station receives the RF signal and demodulates it to extract the original data.

2.2.1 Satellite Networking Protocols

Satellite networking faces unique challenges that are not present in terrestrial networking. Latency is one of those challenges because of the inherent nature of the distances between satellite infrastructure. Bandwidth availability has historically been limited, causing potential congestion and slow data transfer rates. Signal degradation is also a major challenge, including interruption and reduced reliability due to the atmospheric environment in which satellite communications operate [16].

Several solutions have been proposed over the years to deal with these challenges. The Consultative Committee for Space Data Systems (CCSDS) defined a Space Internetworking protocol suite called Space Communications Protocol Specifications (SCPS). The SCPS protocol is based on existing protocols and suites, such as FTP, TCP, and IPSec. For example, SCPS-TP added a set of extensions to TCP to handle the space networking environment, this included high bit error rates, long delays, and significant asymmetries [17].

The SCPS protocols were an early adaption to solve the unique challenges of satellite networking and are still in commercial use even after being deprecated. CCSDS has replaced SCPS with a new suite called Solar System Internet (SSI). The suite is built on two types of networking architecture, the Internet and Delay-Tolerant Networking (DTN) architectures, which interconnect multiple networks [18]. DTN is a generalized end-to-end networking architecture built for communication through highly stressed enviroments [19].

An example of a protocol that is part of the SSI suite is the CCSDS Bundle Protocol(BP). CCSDS BP adopts the protocol described in RFC5050 and makes it

suitable for space communication. The original BP protocol in RFC5050 builds on the DTN architecture and has functionalities such as store-and-forward capabilities, bundle fragmentation, and reassembly [19]. All these functionalities fit well with the challenges in satellite networking. CCSDS BP builds on this and has improvements such as better encryption, authentication, reduced header size, and improved encoding [18]. This makes the protocol safer and more efficient for use in satellite networking.

Continual research is being done on this topic to keep up with the technological advances of satellite communication. A study investigated the possibility of using QUIC, an end-to-end encryption network protocol, for satellite communication. It concluded that QUIC could be a viable solution for satellite communication by implementing a series of mechanisms at the QUIC endpoints, but pointed out that further work needs to be done to investigate the impact of implementing these mechanisms [20].

2.2.2 Radio Frequency Signals and Modulation

Various technologies and techniques are implemented to facilitate data transfer from the ground segment to the space segment in satellite communication. RF signals and modulation are at the center of this process.

Modulation refers to the mechanisms used to carry data on an RF signal, while demodulation refers to the process of extracting data from an RF signal. The results of modulation on a carrier result in a dynamic change to one or more of the amplitude, phase, or frequency of the carrier [21, p. 327]. Modulation has been around for decades and has evolved from primitive analog modulation techniques to advanced digital modulation techniques capable of handling higher bit rates [22]. Digital modulation can take form in many ways:

From [21, p. 329]

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)
- Quadrature Phase Shift Keying (QPSK)
- Bipolar Phase Shift Keying (BPSK)
- Asymmetric Phase Shift Keying (APSK)
- Quadrature Amplitude Modulation (QAM)
- Orthogonal Frequency Division Multiplexing (OFDM)

Modulation techniques have different characteristics and properties. Modulation strategies are usually deployed in satellite communication systems, where multiple modulation and multiplexing techniques are used together according to the needs of the system [23].

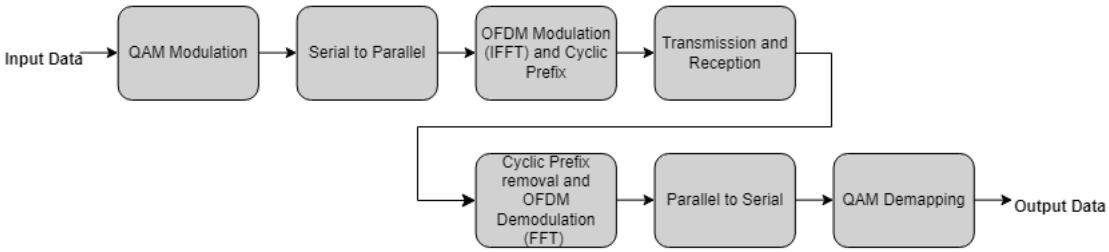


Figure 2.2: OFDM and QAM modulation implementation, based on [24][25]

Figure 2.2 shows a modulation strategy for a satellite communication system that needs to transmit data with high spectral or bandwidth efficiency and robustness.

Radio frequency bands are used in the transmission and reception part of the modulation strategy. Each RF band, divided into their frequency range, provides different types of characteristics and makes the choice of RF band highly dependent on the intended application. For example, the Ku and Ka bands are used for satellite systems that provide low-latency and high-bandwidth Internet [26]. An overview of the most used RF bands, their frequency, typical application and characteristics is presented in table 2.1.

Table 2.1: Overview of the most used radio frequency bands, based on [27]

.

Band	Frequency	Typical Application	Characteristics
VHF Band	30 to 300 MHz	FM radio, analog broadcasting, marine communication systems	Good propagation characteristics
UHF Band	300 to 1000 MHz	Wifi, mobile phones, TV broadcasting	Penetrates buildings, good range
L Band	1 to 2 GHz	GPS, mobile phones, satellite phones	Moderate range and penetration
S Band	2 to 4 GHz	Weather radar, satellite communication	Higher data rates, line of sight
C Band	4 to 8 GHz	Satellite TV, long-distance radio	Moderate atmospheric absorption
X Band	8 to 12 GHz	Radar, satellite communication	High-resolution radar images
Ku Band	12 to 18 GHz	Satellite TV, VSAT, satellite communication	Susceptible to rain fade, high bandwidth
K Band	18 to 27 GHz	Radar, satellite communication	Shorter range, higher data rates
Ka Band	27 to 40 GHz	High-frequency satellite communication	Higher bandwidth, more susceptible to weather
V Band	40 to 75 GHz	Experimental communication, radar	Very high data rates, short range
E Band	60 to 90 GHz	High-capacity wireless communication	High attenuation, short-range, high data rate

2.3 Challenges in Cybersecurity for Satellite Communication

The operation of satellite communications depends on the reliability of the space infrastructure, which includes the cybersecurity aspects. Cybersecurity in satellite communications is more important than ever with the evolving landscape in space and the *New Space Era*. In recent years, there have been multiple studies trying to survey the current cybersecurity landscape of space in general [4], [28], satellite internet [29] [8] and Satellite-based communication [30]. The common theme of these surveys is that research in the field is increasing, but there is still ground to cover in terms of understanding the cybersecurity landscape for space infrastructure in general.

Kavallieratos et al. [4] performed a systematic literature review (SLR) on the state of cybersecurity for each segment of the space infrastructure. The study points out several interesting findings. One of them is that most of the research reviewed focused specifically on the cybersecurity of the satellite and that there is not much attention on the ground and user segments [4]. Another interesting finding is that commercial off-the-shelf (COTS) satellites are expanding the threat landscape significantly and that a lack of standards and regulations poses a significant threat. The study concludes that a comprehensive analysis that includes and combines threats, vulnerabilities, attacks, and risks in all space segments is needed and that a cybersecurity framework should be formulated based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) [4].

Satellite communication systems must deal with the same threats and issues as any cyber-physical system. These systems have to be protected from various threat actors. These threat actors can range from foreign state actors such as military and intelligence all the way to individual hackers and political activists. The threat actors have a varying degree of capabilities and resources, as well as potential motivation [28] [31].

One of the biggest challenges in cybersecurity for space systems in general is the lack of a highly adopted technical cybersecurity standard. Government agencies have been working on the multifaceted challenges of cybersecurity in space systems for a long time, but with the rapid commercialization of the space sector, we see an explosion of space activity from private and civilian owners [32].

Work is being done in this area and cybersecurity recommendations for space are being proposed. The Space Policy Directive-5 (SPD-5) was published in 2020 by the United States. It emphasizes the need for a comprehensive approach to cybersecurity in space and highlights the importance of collaboration between government and commercial actors [33].

NIST is applying its cybersecurity framework to the space domain. This is done through reports that address certain areas within the field. For example, NIST IR 8401 was released in 2023, with the goal of addressing cybersecurity concerns in the ground segment of space operations. The emphasis in this report was on the command and control of satellite buses and payloads [34].

The most comprehensive work is being done by IEEE's S2CY - Space System Cybersecurity Working Group. This group is currently working on a standard named P3349 - Standard for Space System Cybersecurity, where the goal is to define cybersecurity controls for space systems in general [35].

2.4 Satellite Constellations

A satellite constellation consists of a group of satellites that are strategically positioned in orbit around Earth to perform a mission, this can include communication, navigation, and earth observation. Satellite constellations are not a new phenomenon and have been around for decades [36]. Global coverage through a

satellite constellation depends on the constellation's orbital height and the total number of satellites.

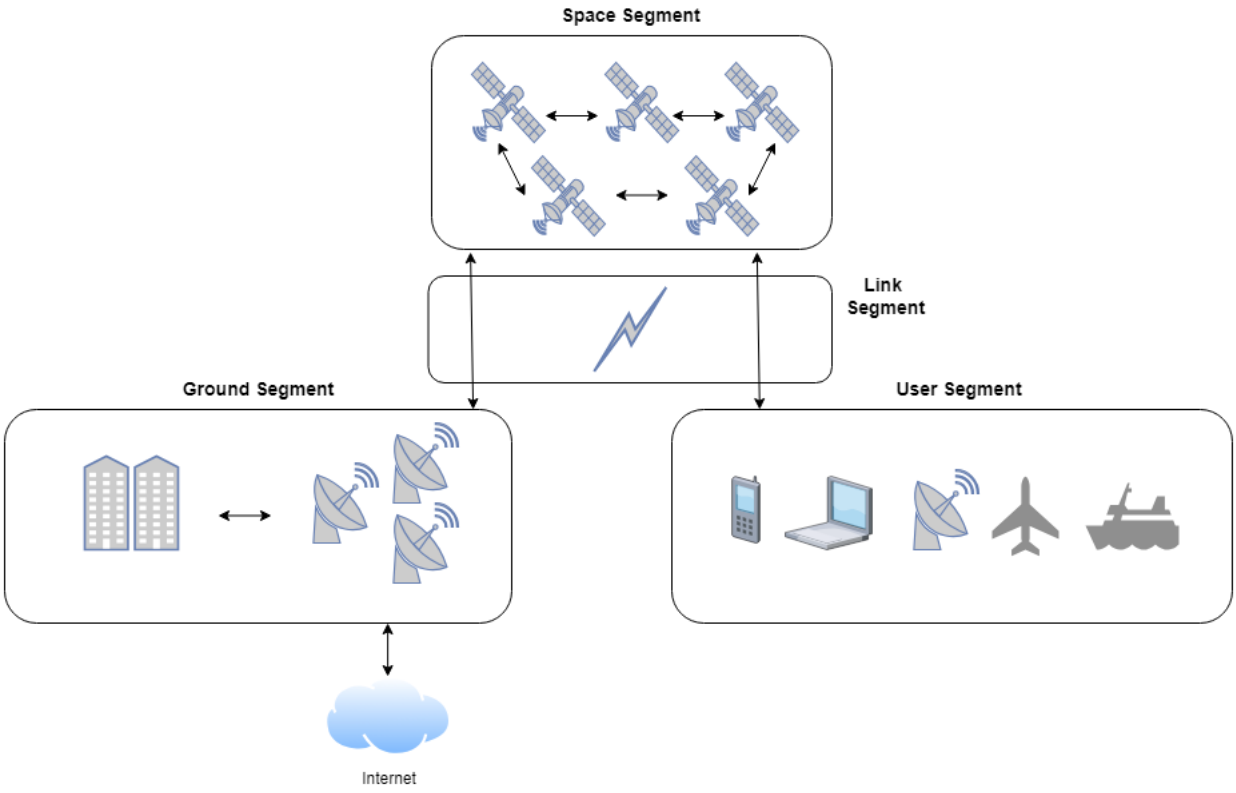


Figure 2.3: Generic overview of a satellite constellation

A generic satellite constellation consists of many moving parts. A simplified overview divided into segments is shown in figure 2.3.

The space segment consists of the satellites and all its components and functionality. The ground segment includes all the facilities and equipment on Earth that are used to control the satellites and process the data they collect. This includes ground stations, control centers, and data processing centers. The link segment entails all communication links between the satellites to and from the ground stations and the user segment, including the communication link from satellite to satellite. The user segment consists of the end user and the end user equipment needed to interact with the satellite system; this includes antennas, terminals, handheld devices, and so on. A more in-depth look at a state-of-the-art LEO satellite constellation, focused on Starlink, is provided in Section 4.2.

2.4.1 Development of LEO Satellite Constellations

There are a number of internet-through-satellite-based companies. EutelSat OneWeb, Intelsat, Telesat, Viasat, Amazon Kuiper, and SpaceX Starlink are some of the

biggest companies in the field [37]. All of these companies are using or are in the process of establishing LEO satellite constellations to provide low-latency and high-bandwidth Internet at an affordable price.

Table 2.2: Overview the most known launched and planned LEO satellite constellation. Based on [9]

Constellation	Number of satellites	Altitude	RF band	Launched
OneWeb Phase 1	648	1200 km	Ku and Ka	Yes
OneWeb Phase 2	Unknown	1200 km	Ku and Ka	No
SpaceX Gen 1/1.5	5313	540-570 km	Ku, Ka	Yes
SpaceX Gen 2	7500 approved	340-614 km	Ku, Ka and E	No
Amazon Kuiper	3236	590-630 km	Ka	No
Viasat	Aprox. 300	1300 km	Ka and V	No
Telesat	198	1000 km	Ka and V	No

Intelsat is currently targeting US government agencies with their LEO satellite solutions, while Amazon Kuiper, Telesat, and Viasat are in the early stages of establishing their LEO satellite constellations. Eutelsat with their Oneweb solution and SpaceX with their Starlink solution are currently the leaders in providing Internet through LEO satellite constellations, at least in the maritime industry [9].

Table 2.3: Starlink and OneWeb performance comparison

	Download	Upload	Latency	Availability
Starlink maritime:	40-220+ MBPS	8-25+ MBPS	<99 ms	$\geq$ 99%
OneWeb maritime:	10-200 MBPS	2-25 MBPS	<99 ms	Unknown(SLA)

From figure 2.3 we can see that Starlink [1] and OneWeb [2] both claim to provide similar performance when it comes to bandwidth and latency. Some of the biggest differences are in the plans and pricing. Starlink sells directly to end users, including companies with simple plans and straightforward agreements. While OneWeb sells their solution to resellers where pricing and other agreements are hard to find.

Another big difference between the two LEO satellite constellations is the altitude at which the satellites operate and the number of satellites in orbit. Starlink has 5313 LEO satellites in orbit that operate from 540 - 570 km above Earth. OneWeb has 648 LEO satellites in orbit that operate at 1200 km above Earth [9]. Both of these characteristics could potentially have an impact on latency and coverage.

During our review of the literature, it became quite clear that Starlink has significantly more research and public information available compared to OneWeb.

[1] Starlink Maritime: `https://www.starlink.com/business/maritime`

[2] OneWeb Maritime: `https://oneweb.net/solutions/maritime`

Because of this, it was decided to focus on Starlinks LEO satellite constellation in this thesis.

2.5 Threat Modeling Frameworks

2.5.1 Introduction to Threat Modeling

Threat modeling has no standardized definition. A systematic literature review of threat modeling concepts from 2023 [38] found a plethora of different threat modeling definition. One of the most accepted definitions is from a 2010 paper [39]: "Threat modeling is a process that can be used to analyze potential attacks or threats, and can also be supported by threat libraries or attack taxonomies".

A review of the literature on threat modeling in 2019 [40] took a systematic approach to identify what threat modeling is and what the state-of-the-art is in this field. This was done by initially analyzing 176 articles, of which 54 of those articles were further analyzed. The paper found that the field of threat modeling lacks common ground and that most threat modeling was still done manually, which was found to be time-consuming and error prone, but that there is a trend towards more automated threat modeling[40].

Threat modeling is often divided into approaches based on the focus of the threat model. There are numerous approaches, but the most common categories found in the literature are software-centric, attacker-centric, and asset-centric. Shostack [41, pp. 34–43] argues that focusing on one approach is preferable to combining approaches because combination tends to be confusing.

Asset-Centric Threat Modeling

Asset-centric threat modeling is an approach to threat modeling with the main focus of identifying and protecting the assets of a system from potential threats [42]. Shostack [41, p. 37] claims that the term asset is commonly used in three ways in the realm of threat modeling. It is things an attacker want, things you want to protect and the stepping stones to either of the two previous descriptions. In general, the approach prioritizes the protection of critical assets by understanding their value, potential threats to the assets, and the possible impact of the identified threat [43].

Attack-Centric Threat Modeling

Attack-centric threat modeling approaches focus on threats from an attacker's point of view [42]. Ucedavelez and Morana [44, pp. 156–159] describe attack-centric threat modeling as an approach to identify which threats can effectively target a system by examining various identified misuse cases, vulnerabilities, available attack vectors, actors, communication channels, and other factors. They further state that the purpose is to address security weaknesses to maintain the application's security and that the analysis is binary, meaning vulnerabilities are either

detected or not detected, allowing for the development or alignment of countermeasures.

Software-Centric Threat Modeling

Software-centric threat modeling attempts to systematically identify, assess and mitigate potential security threats and vulnerabilities within a software system [45]. In doing so, the goal is to anticipate potential threats in the design phase and to design software to counter identified threats.

Shostack [41, p. 43] argues that the preventive nature of threat modeling at the design level and the potential collaboration between software developers and risk management provide a substantial benefit to threat modeling. Shevchenko et al. [46] point out the importance of implementing threat modeling early in a development phase to catch potential issues and implement remedies, potentially preventing those issues later on. They also point out that having security requirements in mind through threat modeling can lead to proactive architectural decisions during the development phase, leading to a reduction of threats [46].

System-Centric Threat Modeling

The three mentioned threat modeling approaches are what we generally see mentioned most in the literature, but there is really no name standardization, and approaches can be named in a variety of ways. Data-driven, security-centric, risk-centric, and more are all examples of threat modeling approaches. There is one more approach worth mentioning and that is system-centric threat modeling.

This approach is similar to software-centric threat modeling. The main difference is that the system-centric approach expands the focus to include the entire system. Software, hardware, network, and environmental components are considered, this includes interaction with users and other systems.

2.5.2 Overview of Prevalent Threat Modeling Frameworks

STRIDE

STRIDE is a threat modeling methodology or framework originally created by Kohnfelder and Garg in 1999 and adopted by their employers Microsoft [3] in 2002 [46]. STRIDE is one of the most mature threat modeling frameworks and stands for *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service,* and *Elevation of Privilege*.

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

Table 2.4: STRIDE categories explained, based on [41, pp. 62–63]

Threat	Property Violated	Threat Definition
Spoofing	Authentication	Pretending to be something or someone other than yourself.
Tampering	Integrity	Modifying data, code or hardware without authorization.
Repudiation	Non-repudiation	Denying having performed an action, making the system unable to prove an action took place.
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it.
Denial of Service	Availability	Making a system or resource unavailable to its intended. users.
Elevation of Privilege	Authorization	Gaining capabilities without proper authorization.

STRIDE has evolved over time, and variants like STRIDE-per-element and STRIDE-per-interaction have been established. STRIDE-per-element focuses on analyzing threats for each individual element of a system, while STRIDE-per-interaction focuses on analyzing threats based on the interactions between different elements of a system [41, pp. 78–85].

The STRIDE threat modeling process is usually divided into four steps in the literature [47]. *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 [41, pp. 44]. *Step 2* consists of mapping the identified DFD elements to the STRIDE threat categorizes. A DFD element can be susceptible to more than one of the categories [47]. The STRIDE threat categories are described in table 2.4. *Step 3* consists in extracting threats. Specific threats are extracted for each of the identified mappings between a DFD element and a threat category. *Step 4* consists of documenting the identified threats in a structured format, this is often done using misuse cases [47].

DREAD

DREAD is an acronym that stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability [48]. DREAD is not a threat modeling framework but a risk assessment framework, but is worth mentioning because it is

often used in conjunction with STRIDE or other similar threat modeling methodologies. DREAD is developed by Microsoft and is used to prioritize and evaluate the severity of threats identified through threat modeling. This is done based on the five factors that DREAD stands for. Each factor is rated on a scale, and the scores are summed to give a total risk score for each threat. This helps in the process of prioritizing threats based on the threats that need the most attention and resources [49].

PASTA

Process for Attack Simulation and Threat Analysis (PASTA) is a comprehensive step by step, risk-centric threat modeling approach proposed by Ucedavelez and Morana in 2012 [46]. The objective of PASTA is to minimize the risk and associated impact on a business based on a seven-step process for simulating attacks and analyzing threats in an application environment. In turn, a business can determine the appropriate level of countermeasures to mitigate the identified risks [50].

The seven steps are:

1. Define objectives
2. Define technical scope
3. Application decomposition
4. Threat analysis
5. Vulnerability and weakness analysis
6. Attack modeling
7. Risk and impact analysis

As mentioned, PASTA is comprehensive and the seven steps are described in detail in [44, pp. 343-478].

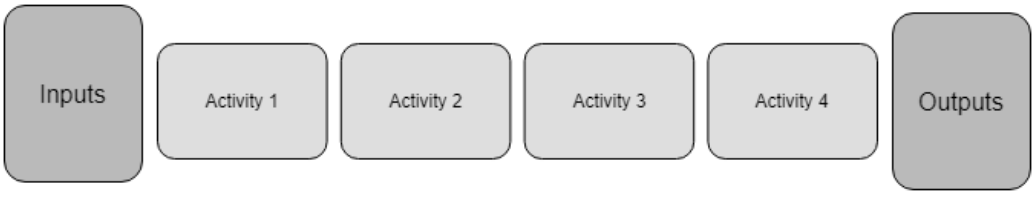


Figure 2.4: Example of actions in a step, based on [44, p. 367]

Each step in PASTA has a predetermined set of actions. A step always starts with inputs. Those inputs are then taken through a set of activities, and at the end of the step we have a set of outputs based on the inputs and activities [50]. PASTA is similar to STRIDE in terms of work flow and steps taken in the threat modeling process. The unique quality of PASTA is that it also takes risk analysis into account, whereas you would have to use STRIDE and DREAD to have the same coverage as PASTA.

LINDDUN

LINDDUN is a privacy threat modeling methodology from 2010 that is based on STRIDE [51]. LINDDUN is an acronym that stands for the seven types of privacy threats it addresses: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, unawareness, and Non-compliance [52]. The threat model consists of six steps divided into two spaces called problem space and solution space [53].

Problem space:

- Step 1: Define DFD
- Step 2: Map privacy threats to DFD elements
- Step 3: Identify threat scenarios

Solution space:

- Step 4: Prioritize threats
- Step 5: Elicit mitigation strategies
- Step 6: Select corresponding PETS

Steps 1-3 are considered the core steps of LINDDUN, because the aim is to identify privacy threats in a system. Steps 1-3 aim to translate the identified threats into viable privacy strategies and solutions that can mitigate the threats [53].

2.6 Specialized Threat Modeling Frameworks

2.6.1 SPARTA

The Space Attack Research and Tactic Analysis (SPARTA) matrix is a framework developed by The Aerospace Corporation to address the information and communication barrier in the space field [54]. 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 represents the tactical goal of the threat actor. The tactic also provides the reason for why they are performing a technique. A total of nine tactics are identified in SPARTA. The nine tactics are: *Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Defense Evasion, Lateral Movement, Exfiltration, and Impact* [55].

Techniques are used to explain how a threat actor accomplishes a tactical objective through specific actions. SPARTA also defines sub-techniques, these techniques represent a more specific instance or variation of the parent technique, giving lower-level details of a technique in a scenario where it would be applicable [56]. Techniques are predefined in SPARTA and falls under one of the nine tactics. 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 [57].

SPARTA also defines countermeasures that can be employed to prevent successful execution of a technique or sub-technique. The countermeasures are made

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

and mapped to standards such as NIST SP 800-53 [5] and ISO 27001 [6]. This is done to provide the user of SPARTA with a more complete understanding of the security principles used, and also helps align SPARTA with potential compliance and regulatory needs [58]. The framework is not necessarily a traditional threat modeling framework, but can be utilized as an attack-centric threat modeling framework by utilizing their navigator tool. An example of SPARTA in use can be found in Section 5.2.

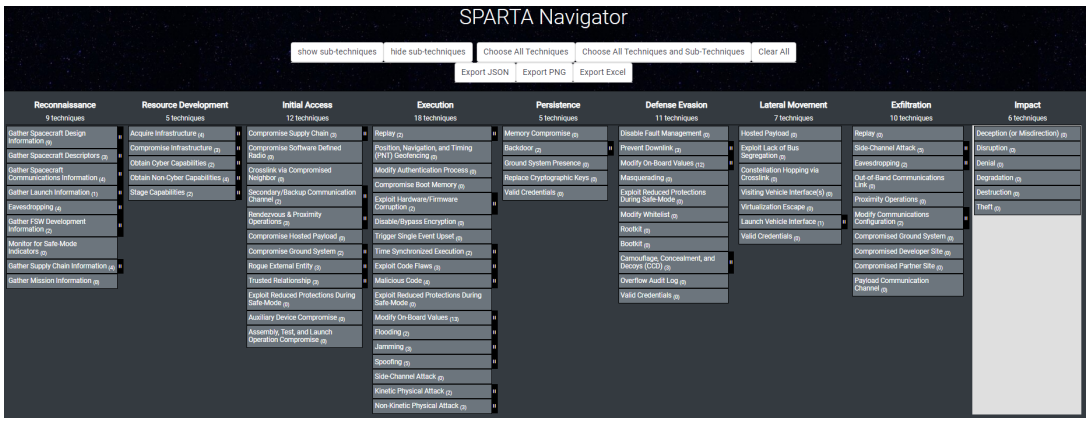


Figure 2.5: Sparta Navigator tool used for attack-centric threat modeling, from [59]

[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`

Chapter 3

Related Work

In this chapter, we review the existing literature related to threat modeling in satellite communications and maritime operations.

3.1 Threat modeling for Satellite Communication in Maritime Operations

This thesis mainly focuses on threat modeling in satellite communication for maritime operations, specifically looking at the recent emergence of high-bandwidth and low-latency LEO satellite constellations, the impact this will have on maritime operations and the use of threat modeling as a tool to identify threats in this area. To the best of our knowledge, there is no prior work that specifically addresses this problem statement. To this end, we structure our related work chapter to cover relevant studies and research on the four segments of satellite communication as explained in section 2.1. The link segment is not explicitly mentioned as this segment is deeply intertwined and covered in the three other segments.

3.1.1 Space Segment

The space segment is one of the most researched segments when it comes to threat modeling, risk analysis, and overall cybersecurity research. There is a clear indicator that this area gets the most attention out of the four segments [4]. 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 [60]. The study focuses on a teleoperation use case. STRIDE and DREAD are used to analyze the efficacy of existing threat modeling methods capability of capturing threats and security requirements from a system-centric approach. A total of 97 different threats were identified. 11 threats were classified as critical and 10 threats were classified as high risk. Possible mitigations were also discussed.

In [61], Hasan and Hasan present a threat model and security analysis of spacecraft computing systems. The paper identifies critical assets in spacecraft systems; this includes on-board computers, communication systems, sensor systems, and command and control systems. STRIDE is used as the threat modeling methodology and they identified threats in line with STRIDE. A mitigation plan for identified threats is also provided. In [62], a novel framework is presented that aims to assess the high-level resilience status of any given space system to any given threat.

Willbold et al [63] developed a taxonomy of threats against satellite firmware, by doing this they could derive satellite-specific threat models. Three real-life satellites were examined based on these threat models and found software vulnerabilities in all of them.

3.1.2 Ground Segment

A range of studies have looked at the cyber security of the ground segment, but there is a gap in terms of threat modeling research in the area. Pavur and Martinovic [28] provide a comprehensive analysis of the historical evolution and current state of cybersecurity threats targeting satellite systems. A satellite vulnerability matrix is developed. The matrix lists vulnerabilities and distinguishes relevance based on segments. The ground segment is thoroughly discussed and points out that general terrestrial IT security approaches are usually used to secure ground segments for space systems.

[64] looks at adopting a methodology for cascading effects analysis on the ground segment of space systems. This is implemented using a model-drive engineering tool. A framework for the detection and estimation of the severity level of physical attack scenarios in the ground segments of space systems is presented in [65].

A comprehensive report on applying the NIST Cybersecurity Framework [1] to satellite command and control is presented in [34]. The report is extensive and discusses cybersecurity on the satellite ground segment as a whole. Threat modeling is identified as an important part in the identification and understanding of existing and future threats. Kinetic physical, non-kinetic physical, electronic, and cybersecurity threats are defined as potential threat modeling categories [34].

3.1.3 User Segment

The user segment of satellite communication is quite broad, in this thesis we focus primarily on maritime operations and more specifically on ships and its satellite communication systems. Kavallieratos et al. investigate cyberattacks against autonomous ships in [66]. The paper identifies the architecture for an autonomous ship, also referred to as a cyber-enabled ship. STRIDE threat modeling is then applied to analyze threats to the identified systems.

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

In [67], Enoch et al. propose a novel graphical security model named MV-HARM. The model is made to systematically capture the security of maritime vessel networks; this includes internal and external networks. A Markov chain-based model for ship cybersecurity management is outlined in [68]. The model tries to take into account the random nature of cyberattacks and applies a mathematical approach to predicting and managing cyber risks on board the ship network infrastructure.

Chapter 4

Methodology

This chapter outlines the thesis research design and justifies the methodological choices made to answer the research questions presented in Chapter 1. It also outlines the two use cases that were used during the project and describes how our chosen threat modeling frameworks were applied to each use case.

4.1 Research Design

One of the main challenges of this thesis is the lack of established knowledge and research done on the specific topic. Threat modeling and risk assessment are areas that have been extensively researched; this includes threat modeling for space systems and maritime operations to some extent. The emergence of modern LEO satellite constellations has put satellite communications in maritime operations back to an infancy stage, because of the possibilities that these LEO satellite constellations provide in terms of cost-efficient, high-bandwidth, and low latency for Internet through satellite communications.

This thesis uses a qualitative methodological approach to answer the research question in Section 1.4. The reasoning behind this choice is found in the literature and in the nature of our research questions. The qualitative research approach has some key features, as outlined in [69].

Table 4.1 shows some key features in qualitative research. One of the main tasks of this thesis is to perform threat modeling in two use cases. These threat models are qualitative, involving the identification, analysis, and description of threats, vulnerabilities, and risks. The use cases in the thesis are directly related to the case study approach of qualitative research, where the focus is to identify the characteristics of a particular entity or system [70].

4.1.1 Research Methodology Applied

The research methodology followed the steps shown in figure 4.1. A literature review was conducted to establish reasonably complete knowledge of the research

Table 4.1: Key Features in Qualitative Research, based on [69]

Qualitative Research	**Description**
Examines	Phenomena
Interpretation	Series of interpretative techniques aimed at describing, decoding, and translating concepts and phenomena, rather than measuring the frequency of these phenomena in society.
Usual selection criteria	• An interpretation is needed. • Research area is relatively new. • Research questions are related to "what", "how", "when" and "where".

situation on the topic. Then the background chapter and the threat modeling review were done on the basis of the literature review. The two use cases were developed after that. Framework selection and application were performed, and threat modeling on the two uses cases was completed, An risk analysis was also performed on use case 1. The results of the threat modeling were analyzed and presented. Finally, all steps were used to answer each research question.

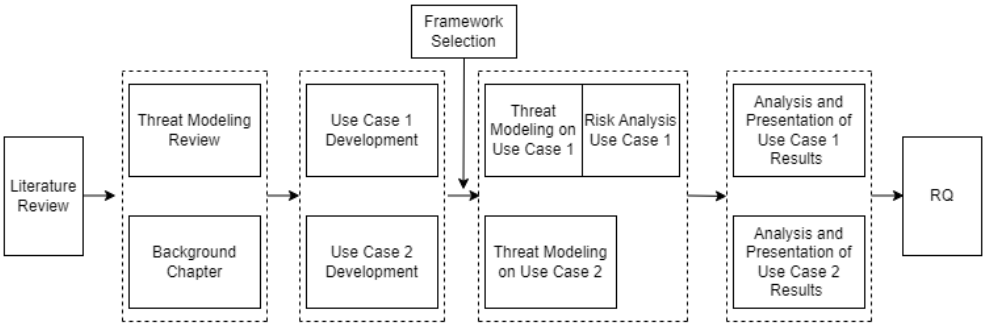


Figure 4.1: Overview of applied research methodology.

4.2 Use Case 1: Satellite Communication

The first use case was developed to provide a high-level overview of a system that uses a modern LEO satellite constellation for Internet through satellite communication. From the literature review and background chapter it became clear that Starlink was the LEO satellite constellation with most adaptation. A large shipping vessel was also selected for the maritime part of the use case because large ships are reliant on Internet through satellite communication to operate in any capacity.

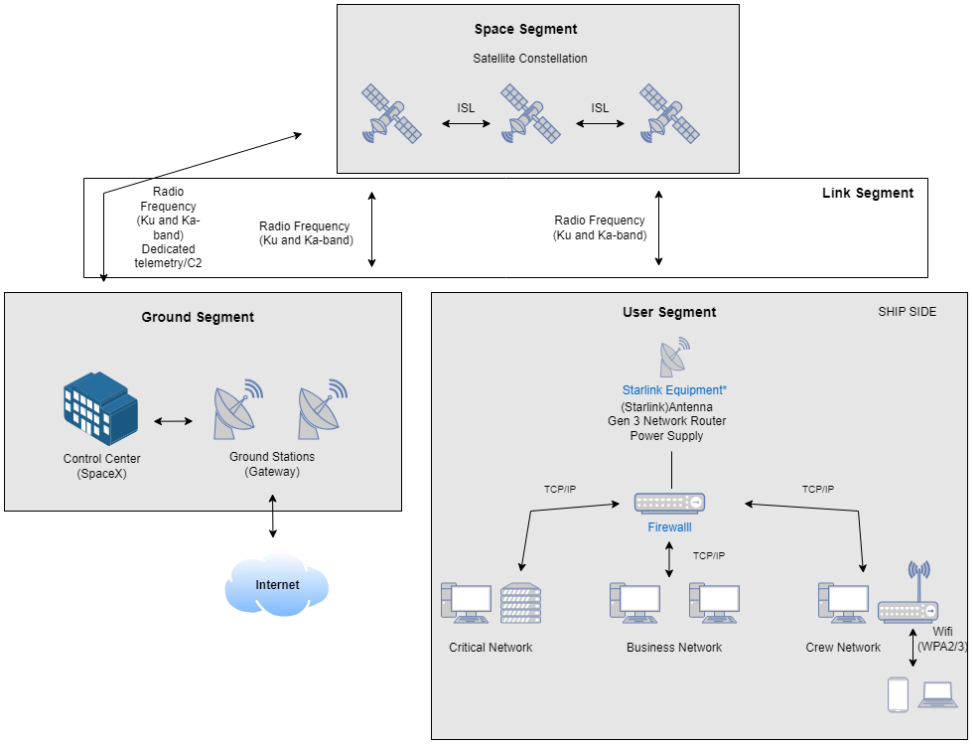


Figure 4.2: Use Case 1: Satellite Communication Overview.

The use case was developed by thoroughly reviewing all publicly available information. This approach presented significant challenges, as companies that offer satellite communication solutions tend to closely guard their technology, architecture, and techniques. Secrecy aside, the publicly available information gave us enough data to formulate a high-level overview of the use case. The use case is depicted in Figure 4.2. The assets of the use case are divided into four segments of the space infrastructure.

4.2.1 Space Segment

For Starlink, the space segment consists of 5313[1] satellites operating at an LEO altitude of 540 to 570 km above earth as of writing this thesis [9]. The satellites uplink and downlink operate in the Ku- and Ka-bands, with a frequency range of 10.7–12.7 GHz, 13.85–14.5 GHz, 17.8–18.6 GHz, 18.8–19.3 GHz, 27.5–29.1 GHz, and 29.5–30 GHz [71]. Satellites have multiple antennas and the ability to connect to multiple terminals at the same time, and according to [72], Starlink uses an OFDM modulation technique for signal transmission. Recently, the OFDM modulation and waveform was confirmed by a patent filed by SpaceX [73]. The first versions of the Starlink satellites used a bent-pipe solution for satellite-to-satellite communication, but ISL has been adapted and tested since version 1.5 of

[1]Starlink SX: `https://starlink.sx/`

the Starlink LEO satellites was launched [37].

4.2.2 Ground Segment

As mentioned in Section 4.2, there is no publicly available information on Starlinks control centers. We can only assume that they operate as a normal command center, 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 [74].

4.2.3 User Segment

The LEO user segment consists of the user terminal and other hardware and software needed. For Starlink this includes [75]:

- Dish: 5.7 kg, electronic phased array antenna, 140 degree field of view.
- Power supply
- Starlink cable
- Ethernet cable
- AC cable

For this particular use case, the user segment also consists of a firewall and three internal networks on the ship. All the networks use generic standardized network protocols.

- Firewall: 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. This 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. This can include stationary computers, laptops, and other relevant devices.
- Crew Network: The crew network consist of the crew wifi network solution and all devices connected to that network.

4.2.4 Link Segment

All components of the link segment have already been mentioned in the 3 previous sections. This includes Ku- and Ka-bands and specialized protocols described in Section 2.2.1.

4.2.5 Threat Modeling Framework

The choice of threat modeling framework to apply to the use case is an important decision in the threat modeling process. For use case 1 we have chosen to use STRIDE. The reason for this is that STRIDE provides a structured and systematic approach to identifying, analyzing, and mitigating potential threats. The use case is broad, with numerous assets in the system. STRIDE is comprehensive and the most mature framework when it comes to system-centric threat modeling. An in-depth explanation of the STRIDE threat modeling methodology is given in Section 2.5.2.

4.2.6 Threat Model Tooling

Correct use of threat modeling tools can improve the threat modeling process by providing a structured, efficient, and comprehensive approach to identify and mitigate threats. Microsoft Threat Modeling Tool (MTMT) version 7.3.31026.3 was chosen as the threat modeling tool for use case 1. MTMT is the most comprehensive STRIDE-specific threat modeling tool.

Figure 4.3: Overview of stencils in Microsoft Threat Modeling Tool [76].

MTMT comes with templates, and SDL TM Knowledge Base (Core)(4.1.0.11) was used as the base template for this thesis. The templates come with predetermined assumptions and descriptions and are usually related towards software-specific threat modeling. This means that we had to modify parts of the template to fit our needs, which is in line with Microsoft's user guide on MTMT [76]. The elements in the DFD are called stencils in MTMT, an overview of the elements can be found in Figure 4.3. The definition of these five elements had to be adjusted in our STRIDE threat model.

Process:

- Original meaning: Any process or action performed by a system. This could be any computational task or operation.
- New meaning: Represents a system component or operational entity involved in the satellite communication process.

External Interactor:

- Original meaning: External entity that interacts with the system, typically a user or an external system.

- New meaning: Represents an external system or network interacting with the satellite communication system. For example, terrestrial internet backbone.

Data Store:

- Original meaning: Any storage location for data, such as a database or file system.
- New meaning: Not applicable in our threat model.

Data Flow:

- Original meaning: Represents the flow of data between processes, data stores, or external interactors.
- New meaning: Represents the flow of data between system component or operational entity involved in the satellite communication process.

Trust Boundary:

- Original meaning: 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.
- New meaning: Used in our threat model, but no need for change in definition.

4.2.7 Risk Analysis

Part of the research questions involved finding the risks associated with the identified threats toward satellite communications in maritime operations. MTMT does not have any built-in future for risk analysis or assessment of identified threats. This meant that we had to implement other measures for our risk analysis of use case 1. Firstly, a manual STRIDE threat modeling process was performed on each identified asset for our use case.

Table 4.2: Stride template based on [66]

SYSTEM				
T	**Threat description**	**I**	**L**	**R**
S		x	x	x
T		x	x	x
R		x	x	x
I		x	x	x
D		x	x	x
E		x	x	x

Table 4.2 shows the STRIDE table that was used for manual STRIDE threat modeling. Column one with "T" (Threat) at the top lists out the STRIDE threat categories subsequently. The cell containing "I" stands for Impact, cell with "L" stands for Likelihood, and cell with "R" stands for Risk.

The risk analysis considered the likelihood of an attack and its impact and was based on [66] and [77, pp. 81–84]. For the manual threat modeling process in our thesis to be feasible, only one threat was identified and used for each category of the STRIDE model. The risk matrix depicted in 4.4 was used as part of the risk analysis, where Table 4.3 was used as impact criteria and Table 4.4 was used as likelihood criteria. This follows the risk analysis from [66].

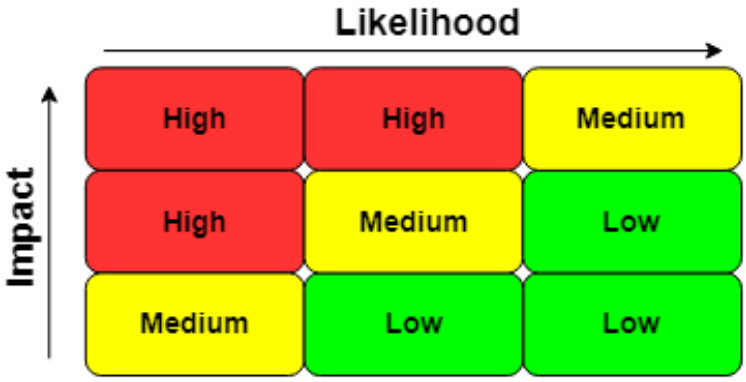


Figure 4.4: Risk matrix, based on [66].

Table 4.3: Threat criteria for satellite communication in maritime operations, based on [66]

Threat 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 4.4: Likelihood criteria for satellite communication in maritime operations [66].

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.

4.3 Use Case 2: Ground Station Attack

The first use case had a holistic threat modeling approach for a comprehensive system. In the second use case, we took specific assets identified from the STRIDE threat modeling and applied a more specific framework for the threat modeling process.

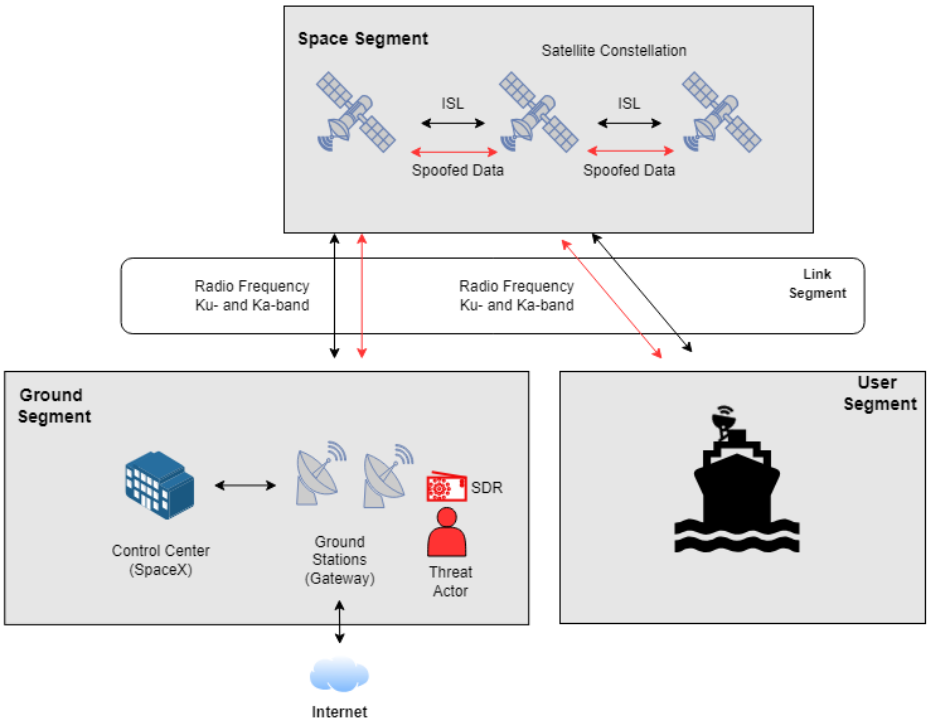


Figure 4.5: Use Case 2: Ground Station Spoofing Attack Through SDR.

In this use case, we explored a sophisticated attack scenario in which a threat actor compromises a ground station connected to the Starlink LEO satellite constellation and uses a software-defined radio (SDR) to spoof GPS signals that are intended for a ship. The use case also explores the possibility of amplifying a GPS spoofing attack by exploiting the satellite constellation hopping feature via Inter-Satellite Links (ISLs). Figure 4.5 shows a topology diagram of this scenario.

4.3.1 Threat Modeling Framework

During our literature review and background chapter, we looked at specialized threat modeling frameworks. SPARTA was identified as a framework that could be used as an attack-centric threat modeling framework. SPARTA was chosen as the framework for this use case because it is specifically designed to address threats in the space domain, which is a critical aspect of our scenario. By utilizing the SPARTA TPPs we got to analyze the tactics, techniques, and procedures used by

the attacker, and gained a better understanding of the attackers perspective. More information about SPARTA is found in Section 2.6.1.

4.3.2 Threat Model Tooling

The SPARTA matrix comes with a suite of tools that made the threat modeling process faster and more effective. One of the key tools is called Navigator [2]. This tool provides a visual representation of the threat model and allows the user to navigate and explore the attack paths and vulnerabilities in a more intuitive way. Figure 2.5 shows the tool. SPARTA also has a tool named Countermeasure Mapper [3], which helps identify and prioritize countermeasures to mitigate the identified threats. In addition, SPARTA has a threat catalog that contains known threats and vulnerabilities in the space domain.

[2]SPARTA Navigator Tool: `https://sparta.aerospace.org/navigator`

[3]Countermeasure Mapper: `https://sparta.aerospace.org/countermeasures/mapper`

Chapter 5

Results

This chapter begins by presenting the findings from the STRIDE threat modeling process. These findings are divided into separate sections, where the results from Microsoft Threat Modeling Tool are presented in one section. Results from manual STRIDE threat modeling, including risk analysis, are presented in the next section. Then the results from the SPARTA threat modeling are presented. These results are divided into sections based on each step or tactic from the SPARTA matrix.

5.1 STRIDE Threat Modeling Results

The STRIDE threat modeling process started by building a DFD-diagram based on the identified assets of Section 4.2, this was done using MTMT. The DFD-diagram is visualized in Figure 5.1.

5.1.1 MTMT STRIDE Threat Model

The threat model produced a total of 177 threats in use case 1. Showing all exported threats would not be feasible for this thesis. MTMT has an export function that provides a report of the threats identified in the threat model. This report gives the following information for each threat:

- ***State:*** Indicates the current status of the threat or mitigation action.
- ***Priority:*** Importance level of the threat.
- ***Category:*** Classifies the threat according to the type of risk it represents.
- ***Description:*** Explanation of the threat, including how it could be exploited.
- ***Justification:*** Proposed mitigation tactics and the reasoning for them.
- ***Short Description:*** Gives a brief threat summary.

A few threats are chosen to show the functionality of the threat model and the export feature in MTMT. Figure 5.2 shows an exported threat in the Denial of Service category, for the RF signal data flow between a ground station and a LEO satellite.

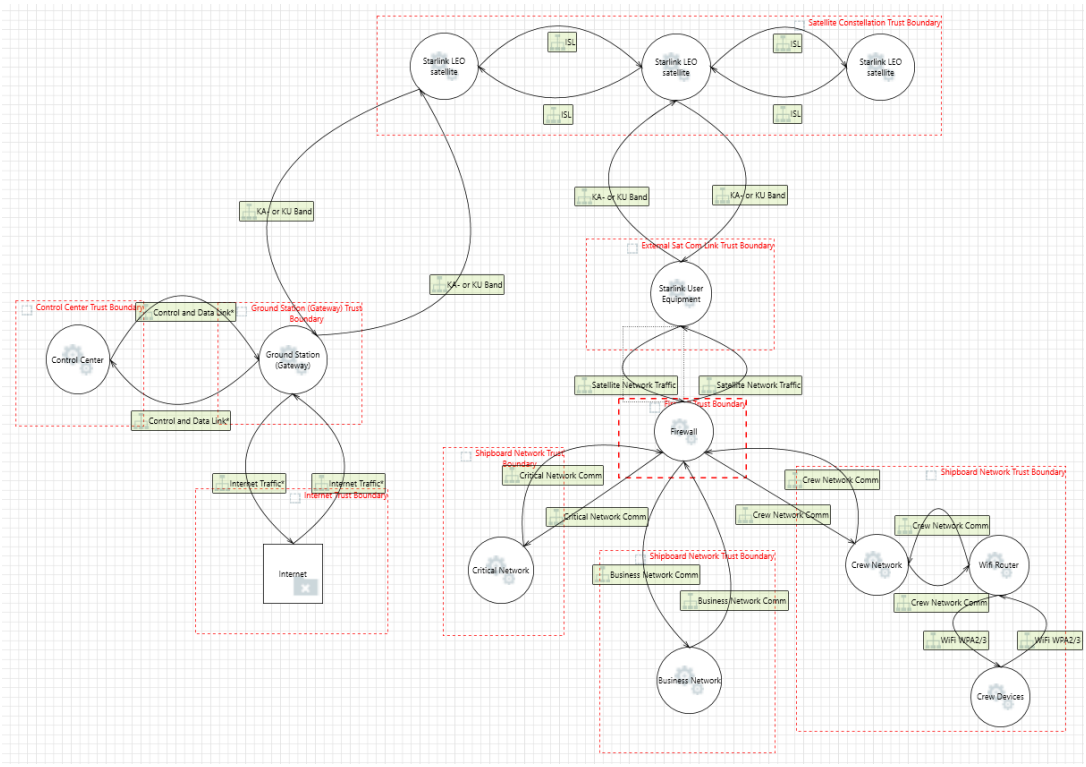
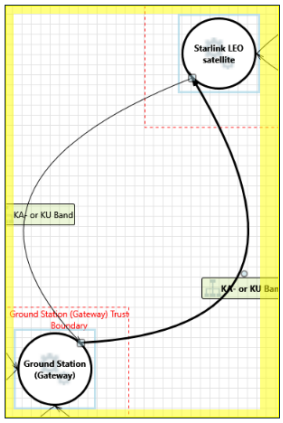


Figure 5.1: Use Case 1: DFD-diagram

Interaction: KA- or KU Band



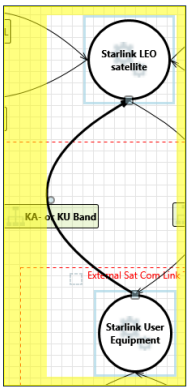
1. Data Flow KA- or KU Band Is Potentially Interrupted [State: Needs Investigation] [Priority: High]

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.

Figure 5.2: Interaction between Ka- or Ku-band for Ground Station and Satellite

Everything except for the justification field is automatically generated by MTMT. This is done based on the template used. The justification for the threat in Figure 5.2 was manually added, but based on research [78]. Figure 5.3 shows an exported threat in the Information Disclosure category, looking at data flow sniffing on the RF signal data flow between Starlink user equipment on the ship and Starlink LEO satellite. The justification field is manually added.

Interaction: KA- or KU Band



2. Data Flow Sniffing [State: Needs Investigation] [Priority: High]

Category:	Information Disclosure
Description:	Data flowing across KA- or KU Band may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.
Justification:	Sensitive information can be exposed on a vulnerable KA- or KU band. This can in turn lead to further attacks on other parts of the system or result in unauthorized disclosure of private or confidential information. Implementation of strong encryption and secure transmission protocols minimize the risk of data flow sniffing.
Short Description:	Information disclosure happens when the information can be read by an unauthorized party.

Figure 5.3: Interaction between Ka- or Ku-band for Starlink User Equipment and Satellite

5.1.2 Manual STRIDE Threat Model

The manual STRIDE threat model was implemented as explained in Section 4.2.7. Tables 5.1 to 5.8 show the results of this process.

Table 5.1: 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 5.1 shows the results of the manual STRIDE threat modeling in the Control Center. 4 high risks and 2 medium risks were identified.

Table 5.2: 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 5.2 shows the results of the manual STRIDE threat modeling on ground stations. 3 high risks and 3 medium risks were identified.

Table 5.3: 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 5.3 shows the results of the manual STRIDE threat modeling on the LEO satellites. 3 high risks and 3 medium risks were identified.

Table 5.4: 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 (Starlink) 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 (Starlink) or network cables connected to Starlink equipment, leading to unauthorized access and data breaches.	H	M	H
D	An attacker could launch a jamming attack on the ship antenna (Starlink, 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 5.4 shows the results of the manual STRIDE threat modeling on the Starlink equipment on board the ship. 4 high risks and 2 medium risks were identified.

Table 5.5: 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 5.5 shows the results of the manual 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 5.6: 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

Table 5.6 shows the results of the manual STRIDE threat modeling in the critical network on the ship. 4 high risks and 2 medium risks were identified.

Table 5.7: 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 5.7 shows the results of the manual STRIDE threat modeling in the business network on the ship. 1 high risk and 5 medium risks were identified.

Table 5.8: 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

Table 5.8 shows the results of the manual STRIDE threat modeling in the crew network on the ship. 5 medium risks and 1 low risk were identified. A consolidation and discussion of the manual STRIDE threat model is found in Section 6.3.

5.2 SPARTA Matrix Results

The SPARTA matrix was applied to the use case described in Section 4.3, where the ultimate objective is to disrupt a ship by spoofing GPS data. SPARTA uses IDs to keep track of tactics, techniques, sub-techniques, and countermeasures. These IDs will be used in the following subsections to make the presentation more readable. Figure 5.4 shows a visualization of the SPARTA matrix applied in our use case.

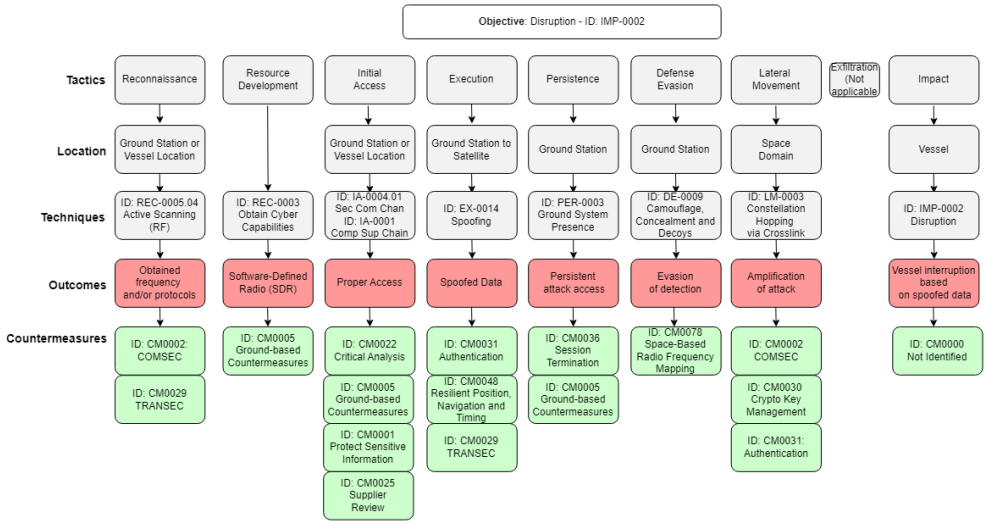


Figure 5.4: Use case 2 visualized in an attack tree format.

5.2.1 Considerations

The SPARTA matrix consists of 9 tactics total. *The Persistence* and *Evasive Action* tactics are combined in our threat model because they have a lot of similarities when it comes to our use case. Tactic *Exfiltration* is not considered because it is not relevant to our scenario. As mentioned, the information presented is adapted from the SPARTA matrix. An overview of the tactics with IDs is found in [55], techniques with IDs in [56], and countermeasures with IDs in [58]. This attack-centric use case is purely hypothetical but is grounded in real-life cybersecurity incidents.

5.3 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.

5.3.1 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.

5.4 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 software-defined radio (SDR) technology and other cyber tools needed to spoof GPS signals.

5.4.1 ST0002 - Countermeasures

Protection of terrestrial assets is in focus to protect from physical attacks on 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.

5.5 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 is:

- **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.

5.5.1 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.

5.6 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 software-defined radio (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.

5.6.1 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 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.

5.7 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 establish 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.

5.7.1 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.

5.8 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.

5.8.1 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.

5.9 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.

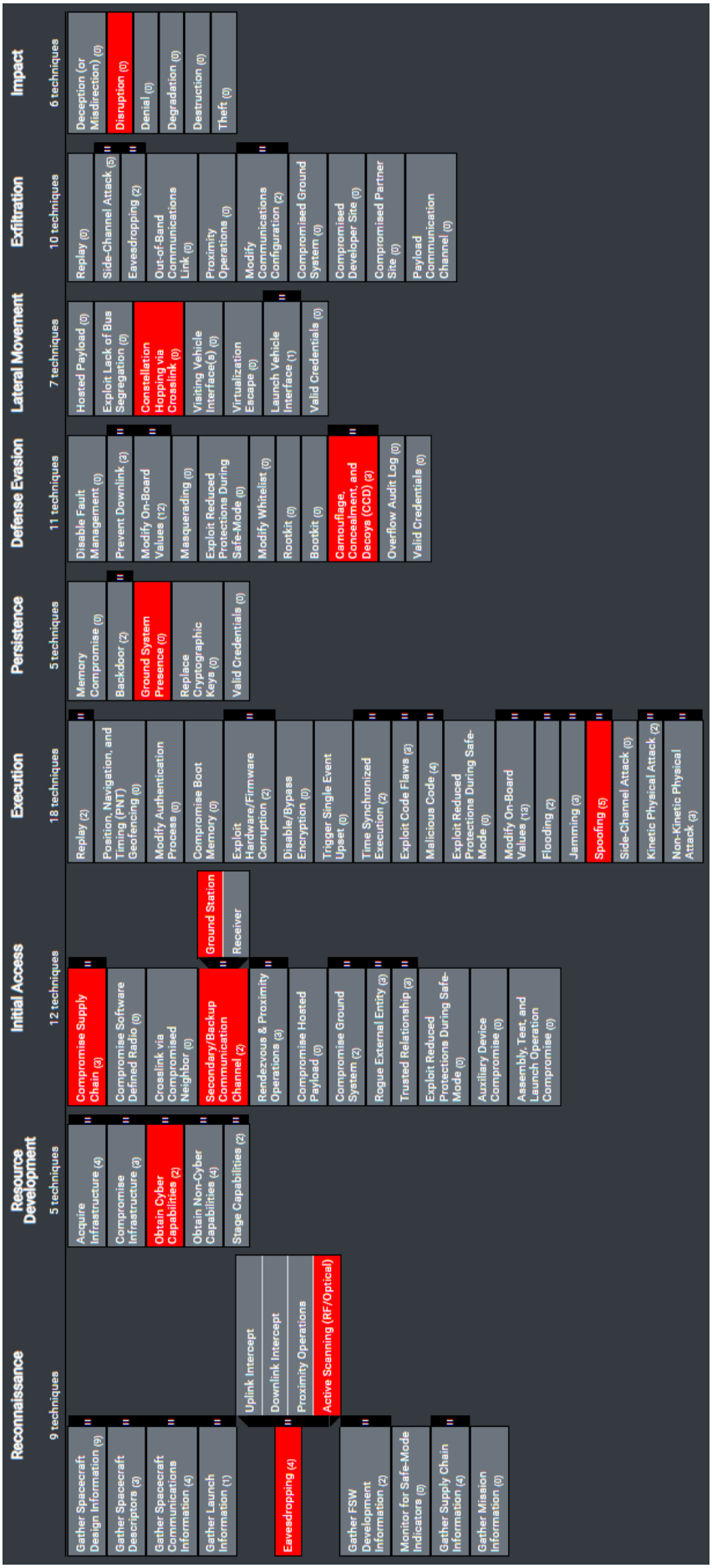


Figure 5.5: Use case 2 visualized in SPARTA Navigator.

Chapter 6

Discussion

In this chapter, the results are discussed in relation to the research questions. Lastly, additional findings and limitations of the research project are presented.

6.1 Research question 1

RQ 1: Cybersecurity in Low Earth Orbit (LEO) Satellite Constellations

- *RQ 1.1: What are the components of a state-of-the-art LEO satellite constellation?*
- *RQ 1.2: What are the cybersecurity threats against LEO satellite components?*

6.1.1 Components of LEO satellite constellations

Satellite constellations have been around for ages, but state-of-the-art LEO satellite constellations are still in their infancy. To date, there are only two private companies that have deployed modern LEO satellite constellations on a large scale, as shown in Table 2.2. For these complex constellations to work properly, they have to have certain components that span across all four segments of the space infrastructure. On top of that, these components have to work in unison. The following sections are based on Starlink specific components as there is a limited amount of data available on state-of-the-art LEO satellite constellation.

The ground segment consists of the components that operate and control the satellite constellation. This includes a control center and strategically placed ground stations. The ground stations also need to be connected to the terrestrial internet backbone. The space segment entails all the satellites needed to provide Internet through the satellite constellation. The satellites operate in LEO, take about 90 minutes to complete an orbit around earth, and weigh approximately 800 kg [7]. The user segment consists of user terminals and other user-related equipment needed to use satellite communication. This includes satellite dishes and antennas. The link segment contains the communication pathways needed to transmit data between the space segment and the ground and user segment. For

a state-of-the-art LEO satellite constellation, this includes Ka- and Ku- RF signals, with custom modulation techniques. A more in-depth explanation of the components in a state-of-the-art LEO satellite constellation is provided in Section 4.2.

6.1.2 LEO satellite component threats

As mentioned previously, LEO satellite constellations are still in the infancy stage and the potential threat landscape is largely unexplored. What we do know is that traditionally all systems that rely on RF signals to communicate are susceptible to signal jamming and interference. Jamming and interference are a major cybersecurity threat due to the low barrier to entry. You do not necessarily have to be a nation state actor with unlimited resources to carry out a successful jamming attack. With off-the-shelf hardware and a primitive attack methodology, a malicious actor would often be successful with a small-scale jamming attack. GPS spoofing is also a regular threat that satellite communications have to deal with, these attacks are usually a bit more sophisticated. LEO satellite components are also vulnerable to the same cybersecurity threat that regular terrestrial systems deal with. Threats and risks are explained and put further into context in Section 6.3.

6.2 Research question 2

RQ 2: What are the most prevalent threat modeling frameworks and what frameworks are best suited for threat modeling for satellite communications in maritime operations?

6.2.1 Prevalent Threat Modeling Frameworks

Several threat modeling frameworks are widely recognized in the cybersecurity domain. These frameworks include, but are not limited to, STRIDE, DREAD, PASTA, and LINDDUN. A high-level overview of these threat modeling frameworks is provided in section 2.5. Each framework offers some unique methodologies for identifying and mitigating threats, catering to different aspects of threat modeling. An interesting observation about the frameworks is that a majority of them base their fundamental approach on STRIDE and are either adding specific steps tailored towards a specific field or application. For example, PASTA is built upon STRIDE fundamentals, but adds a risk assessment component that you would have to use STRIDE and DREAD to get the same coverage.

LINDDUN is also based on STRIDE but is tailored towards a specific application. LINDDUN is applied primarily to identify and mitigate privacy threats and vulnerabilities in systems, particularly those related to data processing, storage, and transmission. Whereas, STRIDE is a more general purpose framework mainly focusing on identifying and mitigating security threats.

The SPARTA matrix is also outlined in this thesis. Although the SPARTA matrix deviates from traditional threat modeling frameworks, it effectively serves as a specialized threat modeling framework with an attack-centric approach.

6.2.2 Suitability for Satellite Communication in Maritime Operations

Satellite communication in maritime operations faces some unique challenges when it comes to threat modeling. Satellite communication systems involve complex, distributed, and dynamic components. Maritime operations, and our focus area ships, also have complex systems onboard, which are often completely reliant on satellite communication to operate.

Our first use case needed a framework that was capable of analyzing the entire satellite communication system, including the LEO satellite constellation, vessel-based satellite equipment, and internal networks, as well as their interactions and dependencies. STRIDE was chosen as the threat modeling framework for this use case because it is a seasoned framework that is able to take a holistic approach to whole systems. The framework also provides customizable tools to help in the threat modeling process, as shown in Section 4.2.6.

The second use case built on the first use case and took a more detailed and attack-centric approach, involving a GPS spoofing attack originating from a ground station, traveling through satellite communication to a target ship. The SPARTA matrix was chosen as the framework for the second use case due to its attack-centric focus and granular analysis capabilities. It also works as a specialized framework because it 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.

For this thesis, STRIDE and SPARTA were used in unison to properly cover an under-researched area and give both a holistic and detailed view on threat modeling.

6.3 Research question 3

RQ 3: What are the identified threats and risks to satellite communications in maritime operations?

A total of 177 threats were produced during our STRIDE threat modeling in MTMT for use case 1. 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 [46].

An overview of the results of the manual STRIDE threat model is provided in Table 6.1. The bottom row of the table shows a total risk score based on the following.

Table 6.1: Overview of manual STRIDE threats and risks, based on [66]

Manual STRIDE overview								
T	**Control Center**	**Ground Station**	**LEO Satellite**	**User Equip-ment**	**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**

TR = Total Risk

- Numerical values given to Red = 3, Yellow = 2 and Green = 1
- All threats from each STRIDE category for each assets is added, giving a total risk score.
- For example, Control Center: 3 + 2 + 3 + 3 + 3 + 2 = 16
- A TR of 15 or higher = Red
- A TR between 10 and 14 = Yellow
- A TR less than 10 = Green

The overview gives us a good understanding of the threats and risks throughout the system. For threats, we can see that Spoofing, Information Disclosure, and Denial of Service scores the highest in terms of 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 compared to Spoofing, Information Disclosure, and Denial of Service. An interesting notion is that these risk results correlate with a similar study done on autonomous ships [66].

The risks for each identified asset in use case 1 are quite high across the board. Business Network and Crew Network are recognized as the assets with the lowest risk, with a total risk score of 13 and 11 respectively. The rest of the assets has a total risk score in the range of 15-16. This makes sense when looking at the functions and importance of the identified assets in the system.

6.4 Use case 2 feasibility

The results of the second use case are presented in Section 5.2. This use case is a purely hypothetical GPS spoofing attack from a Starlink ground station to a vessel via the Starlink satellite constellation. GPS spoofing attacks in itself do not have to be that sophisticated, ships usually have a series of dedicated equipment that uses GPS data. That GPS data are usually provided by a Global Navigation Satellite

System (GNSS). These satellite systems are specifically designed for positioning, navigation and timing (PNT) services and usually operate in MEO.

Research has shown that LEO PNT solutions could be a viable option in the future, when the constellations are fully developed [79]. GPS spoofing attacks targeting a ship are not uncommon, as explained in [80]. We have even seen researcher being able to predict the OFDM modulation technique of the Starlinks RF signals by using of-the-shelf hardware and custom software for signal capture [72].

The most hypothetical part of the GPS spoofing attack used in our scenario is the possibility of amplifying the attack to target multiple ships in an area by abusing the crosslink hopping functionality provided by ISL. This would have to overcome significant technical challenges to become a reality.

6.5 Limitations

The following sections provide an overview of the limitations of this thesis.

6.5.1 Lack of information

One of the main limitations of this thesis is the lack of directly related work in the literature. A broad search, looking for the most related research, was carried out to obtain enough relevant information to complete the thesis in a proper manner. This could have impacted the level of detail of the thesis.

In correlation, space systems, and the field of satellite communication systems, rely on secrecy and proprietary information as a form of security measure. For example, information on the control center and ground stations that operate the Starlink LEO satellite constellation is mostly unknown. The only information available is from the general public, patents, or public filings such as the Federal Communications Commission (FCC) filings. This makes information gathering laborious and significantly prolongs the process.

6.5.2 Research in the field

The advent of high-bandwidth and low-latency Internet through LEO satellite constellation has presented a whole new challenge for the maritime industry when it comes to cyber security. A whole new field is getting more attention from malicious actors because of this new availability. This has caused a significant gap in research and further complicates our work in this thesis.

6.5.3 Threat modeling

There is no threat modeling framework that specifically addresses the maritime industry and the use of satellite communication. This means that we have had to use threat modeling frameworks that are not necessarily the most efficient for our

use cases. The SPARTA matrix is a specialized framework that focuses on space systems and spacecrafts. Tactics, techniques, and countermeasures had to be adapted to be useful in our threat modeling process.

STRIDE also needed to be adapted as there is no template that would work for our use cases. MTMT comes with default templates that are tailored towards a software-centric threat modeling. This meant that we had to take a base template and adjust it to our needs. This becomes time-consuming rather quickly, and the implementation of a truly custom template within MTMT is a worthwhile discussion to have if someone were to adopt this strategy.

The STRIDE threat modeling part where a table template was used had only one threat per STRIDE category, for feasibility reasons. The risk assessment used a rudimentary 3x3 risk matrix that could possibly generalize the risks and not give adequate depth into each of the risks.

Chapter 7

Conclusion

This master thesis aimed to address 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. Three research questions were produced to guide the research and address this threat. These questions involved identifying components and cybersecurity threats towards state-of-the-art LEO satellite constellations, giving a comprehensive overview of threat modeling frameworks and their applicability to threat modeling for satellite communications in maritime operations. In addition, identifying threats and risks to satellite communication in maritime operations.

A qualitative methodological approach was taken to answer these questions by identifying all relevant components in LEO satellite communication and building two use cases for threat modeling based on that information. STRIDE was applied to the first use case, which involved system-centric threat modeling on a complete system for satellite communication to a vessel using the Starlink LEO satellite constellation. The SPARTA matrix was applied to the second use case, which was an attack-centric approach involving GPS spoofing from the ground station, through satellites, and ultimately to a target vessel.

The threat models showed 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. 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. SPARTA showed that a sophisticated GPS spoofing attack can be carried out to disrupt or potentially cause major incidents for ships. By implementing STRIDE and SPARTA in unison, we were able to get significant insight into an area that is currently severely understudied.

7.1 Future Work

Currently, there is no threat modeling framework that meets the unique challenges of satellite communication in maritime operations. A standard Microsoft STRIDE

template was adjusted to fit our needs in this thesis. The development of a STRIDE template for satellite communication would be a step in the right direction.

The manual STRIDE threat modeling and risk assessment from this thesis could be expanded to include more threats per category, and the risk assessment could be expanded further, including a proper risk scoring scheme. This could provide a better understanding of the threats and risks of the system, making prioritization of threats and risks easier.

Both of the use cases in this thesis could be simulated in real-world application to further understand the challenges and possibilities in the threat landscape for satellite communication in maritime operations.

Bibliography

[1] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 70–109, Feb. 2020, ISSN: 1553877X. DOI: 10.1109/COMST.2020.3028247. [Online]. Available: https://arxiv.org/abs/2002.08811v2.

[2] Dark Reading Staff, *Satellite Networks Worldwide at Risk of Possible Cyberattacks, FBI & CISA Warn*, 2022. [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/satellite-networks-worldwide-at-risk-of-possible-cyberattacks-fbi-cisa-warn.

[3] P. H. Meland, K. Bernsmed, E. Wille, J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav*, vol. 15, no. 3, pp. 519–530, 2021, ISSN: 20836481. DOI: 10.12716/1001.15.03.04.

[4] G. Kavallieratos and S. Katsikas, "An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space," *International Journal of Critical Infrastructure Protection*, vol. 43, Dec. 2023, ISSN: 18745482. DOI: 10.1016/j.ijcip.2023.100640.

[5] B. Nejad, *Introduction to Satellite Ground Segment Systems Engineering*. 2023.

[6] Y. Henri and Y. H. Int, "ORBIT/SPECTRUM INTERNATIONAL REGULATORY FRAMEWORK Challenges in the 21st century," 2016.

[7] Y. Borthomieu, "Satellite Lithium-Ion Batteries," 2014. DOI: 10.1016/B978-0-444-59513-3.00014-5. [Online]. Available: http://dx.doi.org/10.1016/B978-0-444-59513-3.00014-5.

[8] R. Wang, M. A. Kishk, and M.-S. Alouini, "Ultra Reliable Low Latency Routing in LEO Satellite Constellations: A Stochastic Geometry Approach," 2023.

[9] A. M. Voicu, A. Bhattacharya, and M. Petrova, "Handover Strategies for Emerging LEO, MEO, and HEO Satellite Networks," *IEEE Access*, vol. 12, pp. 31 523–31 537, 2024, ISSN: 21693536. DOI: 10.1109/ACCESS.2024.3368503.

[10] S. Ma, Y. C. Chou, H. Zhao, L. Chen, X. Ma, and J. Liu, "Network Characteristics of LEO Satellite Constellations: A Starlink-Based Measurement from End Users," 2023. DOI: 10.1109/INFOCOM53939.2023.10228912. [Online]. Available: https://www.space.com/spacex-starlink-satellites.html.

[11] Q. Aderoju, "Global Navigation Satellite System (GNSS) and other geospatial tools for various applications," 2022. DOI: 10.30574/ijsra.2022.5.2.0205. [Online]. Available: https://doi.org/10.30574/ijsra.2022.5.2.0205.

[12] S. Vishwakarma, A. S. Chauhan, and S. Aasma, "A Comparative Study of Satellite Orbits as Low Earth Orbit (LEO) and Geostationary Earth Orbit (GEO)," Tech. Rep. 2, 2014.

[13] Ilcev St. D. and Institute of Electrical and Electronics Engineers., *Highly Elliptical Orbits HEO for High Altitudes and Polar Coverage*. Weber Pub. Co, 2010, ISBN: 9789663353296.

[14] A. P. Trishchenko, L. Garand, and L. D. Trichtchenko, "Three-apogee 16-h highly elliptical orbit as optimal choice for continuous meteorological imaging of polar regions," *Journal of Atmospheric and Oceanic Technology*, vol. 28, no. 11, pp. 1407–1422, Nov. 2011, ISSN: 07390572. DOI: 10.1175/JTECH-D-11-00048.1.

[15] Z. Sun, "Satellite Networking: Principles and Protocols," *Wiley*, 2014.

[16] A. Hylton, N. Tsuei, M. Ronnenberg, J. Hwang, B. Mallery, J. Quartin, C. Levaunt, and J. Quail, "Advances in Modeling Solar System Internet Structures and their Data Flows," in *IEEE Aerospace Conference Proceedings*, vol. 2023-March, IEEE Computer Society, 2023, ISBN: 9781665490320. DOI: 10.1109/AERO55745.2023.10115589.

[17] CCSDS Committee, "Space Communication Protocol Specification(SCPS-TP)," Consultative Committee for Space Data Systems, Tech. Rep., 2006.

[18] CCSDS Committee, "Report Concerning Space Data System Standards SOLAR SYSTEM INTERNETWORK (SSI) ARCHITECTURE INFORMATIONAL REPORT CCSDS 730.1-G-1," Tech. Rep., 2014.

[19] S. Burleigh and K. Scott, "Bundle Protocol Specification: RFC 5050," Tech. Rep., 2007. [Online]. Available: http://www.dtnrg.org.

[20] A. Rodriguez, "Enhancing QUIC over Satellite Networks," Tech. Rep., 2022.

[21] P. T. Thompson, "Satellite Communications Modulation and Multiplexing," Tech. Rep., 2013.

[22] K. Singh and A. V. Nirmal, "Overview of Modulation Schemes Selection in Satellite Based Communication," *ONLINE) ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY*, p. 3, 2020. DOI: 10.21917/ijct.2020.0326.

[23] P. Harati, B. Schoch, A. Tessmann, D. Schwantuschke, R. Henneberger, H. Czekala, T. Zwick, and I. Kallfass, "Is E-Band Satellite Communication Viable?: Advances in Modern Solid-State Technology Open Up the Next Frequency Band for SatCom," *IEEE Microwave Magazine*, vol. 18, no. 7, pp. 64–76, Nov. 2017, ISSN: 15273342. DOI: 10.1109/MMM.2017.2738898.

[24] D. Bala, M. A. Hossain, M. N. Islam, I. Abdullah, and M. S. Alam, "Analysis the Performance of OFDM Using BPSK, QPSK, 64-QAM, 128-QAM & 256-QAM Modulation Techniques," Tech. Rep. 24, 2021, pp. 31–38. [Online]. Available: https://www.researchgate.net/publication/346531243.

[25] S. Namdeo and R. Rani, "Designing and Performance Evaluation of 64 QAM OFDM System," Tech. Rep. 6, 2013, pp. 97–105. [Online]. Available: www.iosrjournals.org.

[26] G. Amendola, D. Cavallo, T. Chaloun, N. Defrance, G. Goussetis, M. Margalef-Rovira, E. Martini, O. Quevedo-Teruel, V. Valenta, N. J. Fonseca, and M. Ettorre, "Low-Earth Orbit User Segment in the Ku and Ka-Band: An Overview of Antennas and RF Front-End Technologies," *IEEE Microwave Magazine*, vol. 24, no. 2, pp. 32–48, Feb. 2023, ISSN: 15579581. DOI: 10.1109/MMM.2022.3217961.

[27] NASA, *9.0 Communications*, 2024. [Online]. Available: https://www.nasa.gov/smallsat-institute/sst-soa/soa-communications/#9.2.1.

[28] J. Pavur and I. Martinovic, "Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight," *Journal of Cybersecurity*, vol. 8, no. 1, 2022, ISSN: 20572093. DOI: 10.1093/cybsec/tyac008.

[29] H. Cao, L. Wu, Y. Chen, Y. Su, Z. Lei, and C. Zhao, "Analysis on the Security of Satellite Internet," in *Communications in Computer and Information Science*, vol. 1299, Springer Science and Business Media Deutschland GmbH, 2020, pp. 193–205, ISBN: 9789813349216. DOI: 10.1007/978-981-33-4922-3{_}14.

[30] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, *Satellite-based communications security: A survey of threats, solutions, and research challenges*, Oct. 2022. DOI: 10.1016/j.comnet.2022.109246.

[31] V.-C. Matei, "Cybersecurity Analysis for the Internet-Connected Satellites," Tech. Rep., 2021. [Online]. Available: http://www.teknat.uu.se/student.

[32] G. Falco, W. Henry, M. Aliberti, B. Bailey, M. Bailly, S. Bonnart, N. Boschetti, M. Bottarelli, A. Byerly, J. Brule, A. Carlo, G. D. Rossi, G. Epiphaniou, M. Fetrow, D. Floreani, N. G. Gordon, D. Greaves, B. Jackson, G. Jones, R. Keen, S. Larson, D. Logsdon, T. Maillart, K. Pasay, N. P. Mantii, C. Maple, D. Marsili, E. M. Miller, J. Sigholm, J. Slay, C. Smethurst, J. D. Trujillo, N. Tsamis, A. Viswanathan, C. White, E. Wong, M. Young, and M. Wallen, "An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action," American Institute of Aeronautics and Astronautics (AIAA), Oct. 2022. DOI: 10.2514/6.2022-4302.

[33] B. Bailey, "Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices," Tech. Rep., 2020.

[34] S. Lightman, T. Suloway, and J. Brule, "NIST IR 8401 Satellite Ground Segment," Tech. Rep., 2022. DOI: https://doi.org/10.6028/NIST.IR.8401.

[35] S2CY - Space System Cybersecurity Working Group, *P3349 - Standard for Space System Cybersecurity*, 2024. [Online]. Available: https://standards.ieee.org/ieee/3349/11182/.

[36] Congressional Budget Office, *Large Constellations of Low-Altitude Satellites: A Primer*, 2023. [Online]. Available: https://www.cbo.gov/publication/59175.

[37] W. Zhang, Z. Xu, and S. A. Jyothi, "An In-Depth Investigation of LEO Satellite Topology Design Parameters," 2024.

[38] P. Lohmann, C. Albuquerque, R. C. S. Machado, P. A. Lohmann, and R. Machado, "Systematic Literature Review of Threat Modeling Concepts," 2023. DOI: 10.5220/0000168400003405. [Online]. Available: https://orcid.org/0000-0002-5644-4167.

[39] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, *A systematic review of security requirements engineering*, Jun. 2010. DOI: 10.1016/j.csi.2010.01.006.

[40] W. Xiong and R. Lagerström, *Threat modeling – A systematic literature review*, Jul. 2019. DOI: 10.1016/j.cose.2019.03.010.

[41] A. Shostack, *Threat Modeling: designing for security*, 1st Edition. Wiley, 2014, ISBN: 9781118809990.

[42] L. Obiora Nweke and S. D. Wolthusen, "A Review of Asset-Centric Threat Modelling Approaches," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 11, no. 2, 2020. [Online]. Available: www.ijacsa.thesai.org.

[43] N. Messe, V. Chiprianov, N. Belloir, J. El-Hachem, R. Fleurquin, and S. Sadou, "Asset-oriented threat modeling," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 491–501, ISBN: 9781665403924. DOI: 10.1109/TrustCom50675.2020.00073.

[44] T. Ucedavelez and M. Morana M, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, 1st Edition. Wiley, 2015.

[45] M. Palanivel and K. Selvadurai, "Risk-driven security testing using risk analysis with threat modeling approach," *SpringerPlus*, vol. 3, no. 1, pp. 1–14, Dec. 2014, ISSN: 21931801. DOI: 10.1186/2193-1801-3-754/FIGURES/15. [Online]. Available: https://springerplus.springeropen.com/articles/10.1186/2193-1801-3-754.

[46] N. Shevchenko, T. A. Chick, P. O'riordan, T. P. Scanlon, and C. Woody, "Threat Modeling: A Summary of Available Methods," 2018.

[47] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requirements Engineering*, vol. 20, no. 2, pp. 163–180, Mar. 2015, ISSN: 1432010X. DOI: 10.1007/s00766-013-0195-2.

[48] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *International Journal of Information Security*, vol. 21, no. 3, pp. 509–525, Jun. 2022, ISSN: 16155270. DOI: 10.1007/s10207-021-00566-3.

[49] K. Ram, M. Rao, and D. Pant, "A threat risk modeling framework for Geospatial Weather Information System (GWIS): a DREAD based study," Tech. Rep. 3, 2010. [Online]. Available: http://ijacsa.thesai.org/.

[50] VerSprite, "Process for Attack Simulation & Threat Analysis," Tech. Rep., 2020. [Online]. Available: https://cdn2.hubspot.net/hubfs/4598121/Content%20PDFs/VerSprite-PASTA-Threat-Modeling-Process-for-Attack-Simulation-Threat-Analysis.pdf.

[51] A. Robles-González, J. Parra-Arnau, and J. Forné, "A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes," *Computers and Security*, vol. 94, Jul. 2020, ISSN: 01674048. DOI: 10.1016/j.cose.2020.101755.

[52] L. Obiora Nweke, M. Abomhara, S. Y. Yayilgan, D. Comparin, O. Heurtier, and C. Bunney, "A LINDDUN-Based Privacy Threat Modelling for National Identification Systems," 2022.

[53] Wuyts Kim and W. Joosen, "LINDDUN privacy threat modeling: a tutorial," *CW Reports*, 2015.

[54] The Aerospace Corporation, *SPARTA: Space Attack Research and Tactic Analysis*, 2022. [Online]. Available: https://sparta.aerospace.org/resources/getting-started.

[55] The Aerospace Corporation, *SPARTA Tactics*, 2022. [Online]. Available: https://sparta.aerospace.org/tactic/SPARTA.

[56] The Aerospace Corporation, *SPARTA Techniques*, 2022. [Online]. Available: https://sparta.aerospace.org/technique/SPARTA.

[57] The Aerospace Corporation, *SPARTA Procedures*, 2022. [Online]. Available: https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix.

[58] The Aerospace Corporation, *SPARTA Countermeasures*, 2022. [Online]. Available: https://sparta.aerospace.org/countermeasures/SPARTA.

[59] The Aerospace Corporation, *SPARTA Navigator*, 2022. [Online]. Available: https://sparta.aerospace.org/navigator-view.

[60] A. T. Sheik, U. I. Atmaca, C. Maple, and G. Epiphaniou, "Challenges in threat modelling of new space systems: A teleoperation use-case," *Advances in Space Research*, vol. 70, no. 8, pp. 2208–2226, Oct. 2022, ISSN: 18791948. DOI: 10.1016/j.asr.2022.07.013.

[61] R. Hasan and R. Hasan, "Towards a Threat Model and Security Analysis of Spacecraft Computing Systems," in *2022 IEEE International Conference on Wireless for Space and Extreme Environments, WiSEE 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 87–92, ISBN: 9781665472807. DOI: 10.1109/WiSEE49342.2022.9926912.

[62] J. Plotnek and J. Slay, "A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems," Tech. Rep., 2022. [Online]. Available: https://www.researchgate.net/publication/370102679.

[63] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space Odyssey: An Experimental Software Security Analysis of Satellites," 2023.

[64] I. Bicchierai, E. Schiavone, and F. Brancati, "Modelling and Assessing the Risk of Cascading Effects with ResilBlockly," in *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 261–266, ISBN: 9781665499521. DOI: 10.1109/CSR54599.2022.9850342.

[65] G. Antzoulatos, "Severity level assessment from semantically fused video content analysis for physical threat detection in ground segments of space systems," Tech. Rep., 2021. DOI: 10.5281/zenodo.5567020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/.

[66] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," Tech. Rep., 2019. DOI: https://doi.org/10.1007/978-3-030-12786-2{_}2.

[67] S. Y. Enoch, J. S. Lee, and D. S. Kim, "Novel security models, metrics and security assessment for maritime vessel networks," *Computer Networks*, vol. 189, Apr. 2021, ISSN: 13891286. DOI: 10.1016/j.comnet.2021.107934.

[68] N. Kaminska, L. Kravtsova, H. Kravtsov, and T. Zaytseva, "Modeling ship cybersecurity using Markov chains: an educational approach," Tech. Rep., 2024.

[69] N. Basias and Y. Pollalis, "Quantitative and Qualitative Research in Business & Technology: Justifying a Suitable Research Methodology," 2018, ISSN: 2414-6722. [Online]. Available: http://buscompress.com/journal-home.html.

[70] B. Njie and S. Asimiran, "Case Study as a Choice in Qualitative Methodology," Tech. Rep. 3, 2014, pp. 35–40. [Online]. Available: www.iosrjournals.orgwww.iosrjournals.org.

[71] C. J. Gerber, "CYBERSECURITY RISK EFFECTS OF STARLINK ON RURAL POPULATIONS IN THE UNITED STATES," 2023.

[72] T. E. Humphreys, P. A. Iannucci, Z. M. Komodromos, and A. M. Graff, "Signal Structure of the Starlink Ku-Band Downlink," 2023.

[73] SpaceX, "Modulation and Waveform Patent," *Patent No: US 12.003.350 B1*,

[74] Starlink, *Starlink Point of Presence*, 2024. [Online]. Available: `https://starlink-enterprise-guide.readme.io/docs/peering-with-starlink`.

[75] Starlink, "Flat High Performance Kit Specifications," 2024. [Online]. Available: `https://api.starlink.com/public-files/specification_sheet_flat_high_performance.pdf`.

[76] Microsoft, *Microsoft Threat Modeling Tool*, 2022. [Online]. Available: `https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-feature-overview`.

[77] S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Anton, and S. Gritzalis, *Computer Security* (Lecture Notes in Computer Science), S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, and S. Gritzalis, Eds. Cham: Springer International Publishing, 2018, vol. 10683, ISBN: 978-3-319-72816-2. DOI: `10.1007/978-3-319-72817-9`. [Online]. Available: `http://link.springer.com/10.1007/978-3-319-72817-9`.

[78] X. Wenyuan, "Jamming Attack Defense," Tech. Rep. DOI: `10.1007/978-1-14419-5906-5`.

[79] G. Singh, "SATELLITE COMMUNICATION CONSTELLATIONS AS SOURCES OF ALTERNATE PNT (POSITION, NAVIGATION, AND TIMING)," Tech. Rep., 2022.

[80] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, *A survey and analysis of the GNSS spoofing threat and countermeasures*, May 2016. DOI: `10.1145/2897166`.

NTNU

Norwegian University of
Science and Technology