Master's thesis

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

Fredheim, Jacob Schjøllert

Attack Path Analysis of Satellites Connected to Critical Infrastructure

Master's thesis in Cyber Security and Data Communication
Supervisor: Sokratis Katsikas
Co-supervisor: Georgios Kavallieratos
June 2024

NTNU
Norwegian University of
Science and Technology

Fredheim, Jacob Schjøllert

Attack Path Analysis of Satellites Connected to Critical Infrastructure

Master's thesis in Cyber Security and Data Communication
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

Title: Attack Path Analysis of Satellites Connected to Critical Infrastructure

Student: Fredheim, Jacob Schjøllert

Problem description:

The cybersecurity landscape for orbital satellites is becoming increasingly hostile due to threats from sophisticated adversaries and advancements in offensive cyber capabilities. Satellites play a pivotal role in supporting terrestrial critical infrastructure, offering services that are integral to the functioning of various sectors, including communication, navigation, and earth observation. The reliance on satellite systems extends to military operations, financial transactions, weather forecasting, and emergency response coordination. This interconnectivity underscores a significant dependency on satellite infrastructure. Given their strategic importance, the cybersecurity community emphasizes the need for developing robust and secure satellites.

This master's thesis aims to address the growing concerns regarding the vulnerabilities of satellites and their interconnection with critical infrastructure, through the five following research questions:

RQ1 What is the current state of cybersecurity in orbital satellites?

RQ2 What are the interconnections between satellites and terrestrial critical infrastructure, and to what degree is the infrastructure dependent on this connection?

RQ3 What is the most appropriate methodology to identify attack paths and assess risk?

RQ4 How can attack paths related to satellites be identified using this methodology?

RQ5 What mitigations can reduce the risks associated with these attack paths?

Approved on: 2024-02-15

Main supervisor: Katsikas, Sokratis, NTNU

Co-supervisor: Kavallieratos, Georgios, NTNU

Abstract

The increasing integration of satellite technology in critical infrastructures introduces a new attack surface to disrupt vital societal functions. This master's thesis aims to investigate the cybersecurity vulnerabilities of satellite systems connected to terrestrial critical infrastructure by: (1) evaluating the current state of cybersecurity in orbital satellites, (2) analyzing the interconnections between satellites and terrestrial critical infrastructure and assess the degree of dependency, (3) identifying the most appropriate methodologies for attack path identification and risk assessment, (4) applying these methodologies to identify specific attack paths targeting satellite systems, and (5) proposing effective mitigation strategies to reduce associated risks. This research employs a systematic literature review combined with an analysis of attack paths and mitigation techniques for satellite systems, contributing to the field of cybersecurity in space.

Acknowledgments

I wish to extend my gratitude to my supervisors Georgios Kavallieratos and Sokratis Katsikas not only for the creation of this project, but also for their valuable insights and expertise leading to the completion of this thesis.

I would also like to thank my fellow students situated in room A172, Bjørn, Fredrik, Kristoffer, Mathias, Matija, Ståle, and Tor Håkon, for contributing to a great work environment and for their amazing comradeship.

Contents

List of Figures

List of Tables

List of Acronyms

ASAT Anti-Satellite.

CISA American Cybersecurity & Infrastructure Security Agency.

Comm.Sat Communication Satellites.

COTS Commercial-off-the-shelf.

CPS Cyber Physical System.

CSIS Center for Strategic and International Studies.

EAS Emergency Alert System.

EO Earth Observation.

GA Ground Antennas.

GNSS Global Navigation Satellite Systems.

GPS Global Positioning System.

GS Ground Station.

ISLs Inter Satellite Links.

ISP Internet Service Provider.

ITS Intelligent Transport Systems.

LEO low Earth orbit.

MAC Medium Access Control.

MCS Master Control Station.

MEO medium Earth orbit.

MS Monitor Staions.

NMC Network Management Center.

OBP Onboard Processing.

OS Observational Spacecraft.

PNT Positioning, Navigation, and Timing.

RLC Radio Link Control.

RS Relay Satellite.

RUS Remote Uplink Site.

SDA Starlink Dish Antenna.

SDLS Space Data Link Security.

SLR Systematic Literature Review.

SPP Space Packet Protocol.

SUS Starlink Uplink Station.

TDM time-division multiplexing.

UOC User Observation Center.

UT User Terminal.

Chapter 1 Introduction

In recent years, the integration of satellite systems with terrestrial infrastructure has become a cornerstone of modern society. These systems are integral to services such as communication, navigation, military operations, weather forecasting, and emergency response coordination. However, the increasing reliance on satellite systems also amplifies the risks associated with their potential compromise. The cybersecurity threats facing orbital satellites are multifaceted and complex, requiring a thorough understanding of the current landscape and the development of effective mitigation strategies.

Research regarding space infrastructure and their cybersecurity condition is readily available and discussed by several researchers. The existing research is in distinction to the goal of this thesis, mostly related to addressing space infrastructures as a critical infrastructure, and not focused on the attack paths towards space infrastructure.

Prominent researcher in the field, Jordan J. Plotnek has published several works on the topic of space systems security [1] [2] [3]. Plotnek argues in his works how a second space race now is prevalent with the rapid deployment of new satellites and space systems that introduce new security risks and vulnerabilities. What was earlier considered to be a military domain, has now become an arena for private actors and commercial interests [4]. Comprehensive studies of the engineering, science, and technology aspects of space security is therefore insufficient according to Plotnek [2].

Pavur and Martinovic have further examined the vulnerabilities of satellites in their paper "SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research" focusing on attacks towards their four considered problem domains; RF-link security, space platform security, ground systems security, and mission operations security. Their analysis of over 100 different satellite hacks shows a trend that adversary's favor ground stations and signals as their attack surface, compared to satellite payloads [5].

Gregory Falco discusses the role of satellites and space assets in critical infrastructure, addressing that while space is not considered a critical infrastructure by the American government, most of the critical infrastructure is reliant on space assets. However, despite the government's effort to improve cybersecurity in critical infrastructure, the space assets receive little focus and recognition according to Falco. Adversaries always seek to exploit the weakest link in a system, and right now space assets are the weakest link [6].

The "Cyber Threat Assessment 2022" is a report published by the Center for Strategic and International Studies (CSIS) highlighting the current threat landscape in space, and acknowledging the most prominent counterspace nations. Namely Russia, China, India, Iran, and North Korea. The report concludes that an increase in counter-space capabilities, both physical, like Anti-Satellite (ASAT) missiles, and electronic and cyber-related, are prevalent [7].

It's a clear consensus from all researchers that cybersecurity in space should be prioritized and improved. David P. Fidler urges the U.S. government to take action and integrate space cybersecurity in their existing cooperation with other spacefaring countries, as well as NATO. Claiming that actions on the national, industrial, and international levels can spread awareness about space cybersecurity, and strengthen policy and industry practices [8].

SmartSat's whitepaper on satellite cyber resilience defines the issue as: "...the recurring ability of a satellite system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from and adapt to high-impact low frequency cyber events." [9]. The whitepaper further introduces a novel space systems resilience taxonomy, containing five different categories; Anticipate, Survive, Sustain, Recover, and Adapt. It is found that implementing more cybersecurity measures can contribute to increase the overall system resilience [9].

Vlad-Cosmin Matei also claims that the current methods to ensure satellite systems' cybersecurity have been proven to be lacking or obsolete [10]. In his thesis regarding cybersecurity in internet-connected satellites, he discovers that satellites are currently transitioning to being internet-connected and therefore an even more important part of global communication infrastructure. Secondly, he discovered that the present security measures will not be sufficient to protect the increasingly connected space sector, especially because increased connectivity poses a more attractive target for adversaries [10].

1.1 Motivation

The motivation behind this research stems from the critical role that satellite systems play in supporting national and global infrastructure. As these systems become more embedded in our daily lives, the impact of their disruption grows more severe. The goal of this thesis is to explore and address the vulnerabilities inherent in satellite systems, particularly focusing on the attack paths that adversaries might exploit. By identifying these paths and proposing mitigations, this research aims to contribute to the development of more resilient satellite infrastructures.

From the pre-project it is said that: Even though we don't notice it, space infrastructure has become an important part of our modern life here on Earth. It is responsible for many of the services we use every day, for example satellite communication, which gives us TV broadcasts, internet, and voice communication. As reliance on these systems grows, so do the risks associated with their failure. Although a multitude of factors can compromise space infrastructure, the threat of cyber-related incidents is prevalent. Space assets have become a fundamental component of critical national infrastructure. As a consequence, the demand for resilient systems is substantial [11]. Knowledge of space infrastructures' status quo in accordance with cybersecurity is therefore of great importance, not only to governments but also to the general public. However, knowledge is not enough. An increasingly hostile threat environment and increasingly vulnerable space systems require resilient space systems [1]. As a response, this master thesis aims to discover and determine the best methodologies and frameworks for identifying attack paths and assessing risk related to critical space infrastructure. Identifying possible attack paths is an important step to be able to build robust and resistant systems. [4]

1.2 Scope and Objective

With this study, research is done in order to answer the five research questions below, which in its entirety aims to understand the cybersecurity situation in satellites, and how they can be protected.

RQ1 What is the current state of cybersecurity in orbital satellites?

RQ2 What are the interconnections between satellites and terrestrial critical infrastructure, and to what degree is the infrastructure dependent on this connection?

RQ3 What is the most appropriate methodology to identify attack paths and assess risk?

RQ4 How can attack paths related to satellites be identified using this methodology?

RQ5 What mitigations can reduce the risks associated with these attack paths?

Regarding the scope of the thesis, the information collected is limited to mostly American and European research. Despite both Russia and India being prevalent in the space domain, information about their technologies is scarce and often unavailable in English. Concerning interconnections between satellite systems and critical infrastructure, only the critical infrastructure sectors with direct interconnections to satellite systems are considered for the analysis.

1.3 UN Sustainability Goals

Ensuring the cybersecurity and functionality of satellites that provide crucial services to critical infrastructure is relevant to several UN Sustainable Development Goals. The problems this thesis aims to solve are mostly related to UN goals 9 and 11.

Goal 9 is to: "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation" [12]. This is directly applicable to this thesis, as the ultimate goal is to enhance the cybersecurity of satellites that provide crucial services to critical infrastructure, thereby helping to create more resilient and reliable infrastructure.

Goal 11 involves making cities and human settlements resilient, which this thesis through the protection of critical infrastructure, also aims to do. One can argue that goal 13, which regards climate action, also is considered by this thesis through Earth Observation satellites that provide climate monitoring and can help with climate disaster management. Climate monitoring is an important part of climate research that aims to combat climate change [12].

1.4 Structure

The thesis is structured as follows. Firstly, a description of the utilized methodology will be provided in chapter 2. Further, research question 1 regarding satellite securities state of the art, is answered in chapter 3. Chapter 4 identifies the interconnections between satellites and critical infrastructure in order to answer RSQ2. The attack path analysis methodology is described and identified in chapter 5, and later used in an attack path analysis in chapter 6. To answer the last research question, chapter 7 provides a mitigation framework and corresponding controls. Finally, the results are discussed, and conclusions are drawn in chapter 8.

Chapter 2 Methodology

This chapter provides an overview of the techniques and methodologies used to answer the research questions presented in the Problem Description.

To answer the first two, RQ1 and RQ2, a systematic literature review will be conducted. A Systematic Literature Review (SLR) is described in [13] to provide a high-level overview of a specific research question. It differs from a normal literature review by being more specific and focused towards answering a concrete question by using clear and defined criteria on how to conduct the review. The criteria defined for the SLR conducted in this thesis are mostly restrictive toward the sources and research material used. For research question 1, which aims to describe the state of the art of cybersecurity in space, only research that is maximum 5 years old is considered. This is to obtain relevant and appropriate results. Further, not much complex or extensive googling or digging will be done, because simple and general search terms will provide popular results, and therefore reflecting the state of the art and relevance of cybersecurity in space infrastructure.

The SLR requirements for research question 2 will not be as strict as RQ1, because information and research regarding connectivity between satellites and critical infrastructure might be limited. Only European and American resources are considered because information about Russian and Chinese space infrastructure is not provided in English, and also tend to be more confidential.

A literature survey will be done to answer research question 3, which involves identifying a suitable methodology for analyzing attack paths in satellite systems. Such a survey involves identifying potential attack path methodologies, and determining which would be most applicable for satellite systems. Consecutively, a comprehensive description of the chosen attack path methodology is presented. In chapter 6, the identified attack path methodology will be utilized in practice to assess and analyze potential attack paths in the satellite systems chosen in chapter 4 .

Further, a similar approach as in chapter 5 , a literature survey is conducted to determine an applicable framework for mitigating risk in the satellite system attack paths, hence, answering research question 5. An assessment of available mitigation techniques and frameworks will be done, and the most suitable will be applied in practice.

Chapter 3 State of the art

This chapter aims to answer the first of five research questions discussed in this thesis; "What is the current state of cybersecurity in space infrastructure?".

3.1 Cybersecurity Recognition

Professionals and researchers have long stated the importance of adequate cybersecurity defense in space systems. The idea of cybersecurity in space has however remained relatively unspoken. At least by the general public. Google search statistics show no increase in the search “cybersecurity in space” in the period 2004-2024 as seen in figure 3.1. These searches originate mainly from USA and India. In comparison the term “cybersecurity” is a lot more popular. This is visualized in figure 3.2 where the red line represents “cybersecurity”, and the blue line “cybersecurity in space”. Contrary to the first search, “cybersecurity” is googled all around the world [14].

A tipping point is prevalent. Jacob G. Oakley states in his book *Cybersecurity for space* that: “We are currently at a precarious position in the evolution and accessibility of space operations to academic, commercial, and government entities. More and more computing platforms are being launched into orbit and beyond. Unfortunately, these systems, as a necessity, have a heavy focus on functionality, and

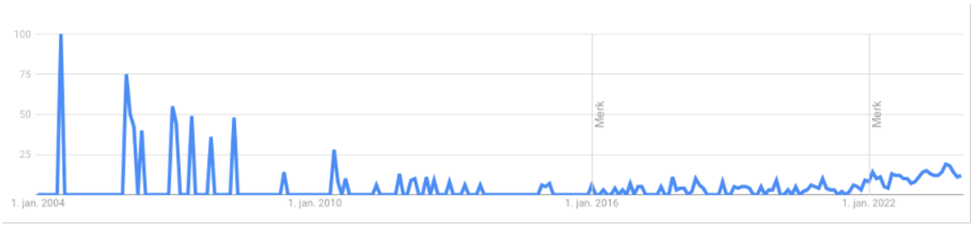


Figure 3.1: Cybersecurity in space [14]

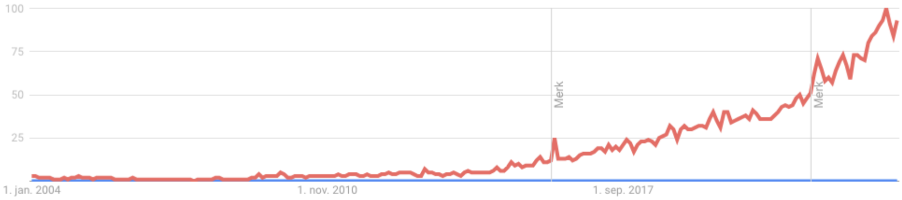


Figure 3.2: Cybersecurity VS. cybersecurity in space [14]

any regard to cybersecurity is oftentimes a byproduct of attempts at safeguarding the space system from failure and not any malicious intent." [15] Oakley implies through this statement that the focus on cybersecurity in space systems is wrong and that it in reality is a trust-based system. He further explains that there exist several adversaries willing to break this trust, and mentions hacktivists, cybercriminals, nation-state actors, and commercial competitors [15]. A solution is required.

In accordance with Oakley's idea that the cybersecurity aspects of space systems are trust-based, is the paper published on behalf of the MITRE corporation by Samuel S. Visner and Peter Sharfman, *Development of Cybersecurity Norms for Space Systems*. Visner and Sharfman here state that: "While some limited cyber-attacks have likely occurred, as of the end of the summer of 2021, there has never been a publicly acknowledged cyber-attack against a space system. We can therefore say that a norm exists that such attacks should not take place – or at least that any cyber-attacks against a space system should be limited to those that will be kept secret not only by the attacker but also by the owner of the target. However, the previously mentioned trends toward proliferation of both space systems and cyber-attacks mean that this norm is fragile.» [16]. Visner and Sharfman support Oakleys theory about how the cybersecurity domain in space systems is trust-based, by defining it as a norm. They state that there exists a norm implying that attacks should not take place. However, they share the same concern as Oakley, that this norm is fragile, and adversaries are willing to play outside rules and norms.

As discussed in the pre-project a change in stakeholders and actors in the space domain is prevalent. What was once a military and state-funded domain, has now been privatized and capitalized [4].:

"Traditionally, space security has been regarded as a military domain. However, a shift in domain owners is becoming more prevalent, as we witness the beginning of a second space race. Private organizations are joining the field, and satellites and rockets are being sent up with a frequency like never before. Billionaires and founders of big tech companies are rushing to take part in the space race. Like Elon

Musk with SpaceX, Jeff Bezos (founder of Amazon) with Blue Origin, and Mark Zuckerberg with his interstellar probe project: “Breakthrough Starshot”. Actors with profit margins in mind can cause trouble in terms of security. » [4]

M. Manilus (et. Al.) introduce the term “Old Space” and “New Space” describing military control and the privatized domain respectively [17]. Several researchers claim that the “New Space” era brings with it the same cybersecurity threats that exist in the IT industry. M. Manilus himself states that; “The change in the economics of space to one which is profit-driven has prompted R&D to have a quicker turnaround with smaller agile teams, mirroring the IT industry rather than traditional aerospace or military outfits” [17], implying that the focus has shifted from national security to profit margins and that this change is substantial. Kaspersky Labs confirms this suspicion and writes on its website that: “transferring today’s IT industry to space brings with it all of the IT industry’s problems” [18]. M. Manilus’ exact definition of “New Space” is: “This agility pattern born from incorporating standard modules and components whilst making space travel cheaper and more widespread across industries is characterized by the term “New Space” [17].

3.2 Geopolitical Differences

It is however important to note that states and militaries still control a huge part of the space domain. Kai-Uwe Schrogl even claims that “space has never been more elaborately used for military and security purposes on earth” in his Handbook of space security from 2020 [19]. The combination of different stakeholders with different agendas makes the space domain more complex than ever. With this increasing utilization of space and space infrastructure, our dependence on the technology and services derived from it grows. Ensuring the integrity and availability of these services is therefore of great importance. Schrogl has even gone so far as to say that: “Space security is a key factor for survival.» [19]

USA, as one of the most powerful nations present in the space domain [20], has begun acknowledging the importance of cybersecurity in space systems. In the President signed Space Policy Directive from 2020 [21], it is said that: “Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation’s critical infrastructure.” [21]. Underlining the importance of robust and functional space systems, the policy further argues that the systems are dependent on wireless radio-frequency communication, which is vulnerable to malicious activities like denial of service and disruption. It is further proposed that space systems and their supporting infrastructure should be developed using risk-based, cybersecurity-informed engineering, because the cybersecurity principles that apply to terrestrial systems also apply to space systems [21].

3.3 Existent Vulnerabilities

To what extent are the demands from the American Space Policy Directive met when designing and producing today's satellites? The results from *Cybersecurity Analysis for the internet-connected satellites* by Vlad-Cosmin Matei show the gap between the desired and actual security. Matei mentions several major vulnerabilities in current satellite systems. One of these vulnerabilities is the lack of authentication. Matei found that many active satellites still have flawed- or no authentication mechanisms, which adversaries can use to gain unauthorized access and issue false commands. [10]. Traffic between satellites and ground stations was also found to be unencrypted in some instances, posing an opportunity for adversaries to intercept messages and compromise confidentiality. Further, satellites' inability to manage incoming signals properly makes them vulnerable to Denial-of-Service and jamming attacks. The importance of secure ground station devices is also discussed, as they compose a necessary part of a space system. Ground stations can be attractive points of attack for an adversary, and Matei claims that ground station devices are no different from devices used in a large-scale company, and therefore susceptible to all usual cyber attacks.

Matteo Calabrese extends the list of known vulnerabilities in his Master's Thesis *Space Oddity: Space Cybersecurity Lessons from a Simulated OPS-SAT Attack*, claiming that the computing power in space systems doesn't bear comparison with terrestrial computing power, much because of constraints related to size, power, and environment. Consequently, crucial security measures like authentication and encryption are often neglected. Antivirus programs, Intrusion Detection- and Prevention systems are according to Calabrese unavailable for securing spacecrafts. He also identifies the cost-related issues with space missions and satellites, where significant expenditures lead to a lower priority for cybersecurity [22].

The thorough investigation of Gregory Falco in his paper *The Vacuum of Space Cybersecurity* discusses how the cybersecurity challenges of the space domain are unique. Because of this uniqueness, engineers believed that the technology was too advanced for hackers to compromise, practicing "security through obscurity" [23]. This principle has later been proven weak. Falco however, explains how the change from analog to digital space assets introduces several cybersecurity challenges, no longer protected by obscurity. Highlighted in the paper is how space systems pose a single point of failure for the terrestrial services and infrastructure they support. "The ability to impact multiple systems by compromising a single space system makes for an attractive target. » [6]. Lack of cybersecurity standards and regulations for satellites affects both the security of legit satellites and the security against malicious satellites. “At this point, there are no agencies that restrict the use of satellites and there is no overarching governing body that monitors the specific use of satellites. Even if one did exist, there are no mechanisms for enforcing any treaties/standards/governance. Because of this, it is possible that some satellites are being used as a base to launch cyber operations or for other nefarious means.” [6].

Another cybersecurity concern is the complex supply chain of satellites. Satellites are composed of multiple different components, often produced by several manufacturers. Each vendor and manufacturer provides an additional opportunity for a hacker to compromise a satellite. Approval processes for these vendors are focused on physical quality control and not cybersecurity. “Unlike most critical infrastructure sectors, space assets are not owned by the same organizations that manage the infrastructure which results in questions related to liability if they are attacked.” [6]. The financial and operational responsibility for cybersecurity in satellites is hard to determine, and as a result, may be neglected. Adding to this issue is the increasing use of Commercial-off-the-shelf (COTS) technology. COTS is often used in low-cost satellites making them relatively cheap to build and launch. The widespread use of COTS has 3 main problems according to Falco. Firstly, the wide availability of COTS products means a lot of people have access to the devices and can analyze them for vulnerabilities. The second challenge is maintaining and upgrading the products to have the latest security patches, which, according to Falco, seldom is done by users. At last, Falco raises skepticism towards the open-source technology behind COTS, arguing that anyone can contribute to the code and therefore might contain intentional vulnerabilities and back-doors. Vulnerabilities in low-cost satellites using COTS may not seem like a substantial problem, as they often are launched by private organizations or hobbyists. However, the severity increases when learning that governments often lease bandwidth from private and commercial satellites. By doing so the vulnerabilities that exist in these satellites are incorporated into military or other government agency IT systems [6].

Kapalidis et al. argues in their paper on Cyber Risk Management in Satellite Systems that the definition of security in space systems depends on how stakeholders are interested in protecting a system. The traditional CIA-triad (Confidentiality, Integrity, and Availability) is expanded to include Authenticity and Safety to ensure a robust space ecosystem. Authenticity is crucial because communications between satellites and ground stations must be genuine and devoid of malicious intent. Additionally, safety considerations are paramount due to the physical nature of satellites; cyber breaches could potentially result in physical harm. [24]

Despite existing regulations recommending a de-orbiting limit of 25 years after deactivation [25], satellites often considerably exceed this limit. This poses a vulnerability, as dormant satellites can be hacked and re-activated by adversaries, without the operator's control or knowledge. Considered as nothing more than space debris, these rogue satellites can function undetected, and therefore cause great harm [24].

High upgrading costs and satisfied customers are factors that cause space operators to still rely on legacy software in many satellites [26]. In addition, many satellites in orbit today have been active for an extensive period. It is therefore evident that some space systems are operating on decades-old software, which is almost certain to contain vulnerabilities and bugs. Compatibility issues between Information and Operational Technology (IT and OT) are also raised by Kapalidis as a vulnerability, as combining the two can reintroduce previously identified bugs [24].

3.4 Implemented Countermeasures

Existing literature primarily emphasizes the lack of cybersecurity measures in satellites, rather than examining the controls that are in place. This could be due to the absence of existing controls in today's satellites. Adrian Schalk has identified what he claims to be the only cybersecurity measure built into the satellite architecture [27], the Space Data Link Security (SDLS). It is a part of the Space Packet Protocol (SPP), which was built to be a reliable communication standard for satellite communication. The SDLS is however optional to implement, and the protocol's security strategy is described as follows; ”The SPP does not provide any security function. Nevertheless, security functions (authentication, confidentiality, integrity) can be implemented either at the data link layer using Space Data Link Security (SDLS) protocols or at the network layer using Bundle Security Protocol” [27][28]

Chapter 4 Satellites and terrestrial infrastructure

In this chapter the criticality of the links between orbital satellites and terrestrial critical infrastructure is explored to answer research question 2; "What are the interconnections between satellites and terrestrial critical infrastructure, and to what degree is the infrastructure dependent on this connection?".

4.1 Critical Infrastructure

Critical infrastructure is defined by the American Cybersecurity & Infrastructure Security Agency (CISA) to consist of: "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." [29]. The definition of critical infrastructure is subjectively dependent on what a country considers as its most important assets and systems. In the 2008/114/EC council directive by the EU, the following definition is given: "'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;", where "Member States" describes the nations present in The European Union. [30] To keep the research in this thesis as objective as possible, a broader more general definition derived from the EU's suggestion is used: "Critical Infrastructure means an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions."

The following 11 sectors is defined by EU in the NIS2 directive to be of high criticality: Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking Water, Digital Infrastructure, ICT Service Management, Public Administration, and Space [31].

Despite the general definition and the EU's defined sectors, the 16 sectors defined by CISA are considered to conduct this analysis, because space is not a part of them. Included in CISA's definition are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems sector [29].

4.2 Interconnections

This chapter will provide an overview of the interconnections between the 16 critical infrastructure sectors mentioned in 4.1 and orbital satellites. Interconnection is defined by the U.S. government in [32] as "the linking of two networks for the mutual exchange of traffic." In the context of this thesis, interconnection therefore describes the link between a satellite system and a critical infrastructure sector. Further in this chapter a thorough investigation of each critical infrastructure sector is done in order to identify possible interconnections to satellite systems. Each sector is then listed with their corresponding satellite system interconnections in table 4.1 . Five different satellite systems are considered: GPS Satellites, Earth Observation Satellites, Communication Satellites, Broadcast Satellites, and Internet Satellites.

4.2.1 Chemical Sector

The chemical sector consists of chemical facilities and distributors that manufacture, store, transport, or deliver chemicals along a global supply chain [33]. Containing mostly manufacturing and transportation, this sector is mainly dependent on satellites for transportation services, like GPS, location, time, air traffic, and sea navigation [34]. In addition, G. Sutlieff et. al. has discovered that satellite data can be used for Chemical, Biological, Radiological, and Nuclear threat detection, monitoring, and modelling. This includes using satellites to discover dangerous chemical and gas leaks, that might be invisible to the human eye. As a result, the chemical sector is interconnected to both GPS and Earth Observation Satellites.

4.2.2 Commercial Facilities Sector

The commercial facilities sector consists of eight different subsectors related to entertainment, shopping, business, and lodging [35]. Regarding satellite connection, the main area of interest is the entertainment and media subsection. Broadcasting of media and entertainment is enabled by geostationary satellites to provide live news, sports, concerts, and other events [36]. Without satellites broadcast media as we know it would not be possible, to this extent, satellites are considered to be critical for the operation of broadcast media. This sector is therefore interconnected to Broadcast Satellites.

4.2.3 Communications Sector

The Communications sector is proclaimed to provide an "enabling function" for other critical sectors and is therefore considered critical in itself [37]. Figure 4.1 shows the Communications Sector's architecture and its services. It depicts five different ways the available services are provided through different access networks. Two of them, Broadcasting and Satellite, rely on satellites to function, indicating that this sector is heavily reliant on satellites. This is also clear from the different services and applications, where GPS, Tracking, Timing, and Satellite radio are listed. Lieutenant Colonel Justin D. Ellsworth emphasized satellites' significance stating that: "Space is buried as a key sub-component within the communications sector," [38]. Hence, this sector relies on several satellite constellations, including GPS, Broadcast, and Communication Satellites.

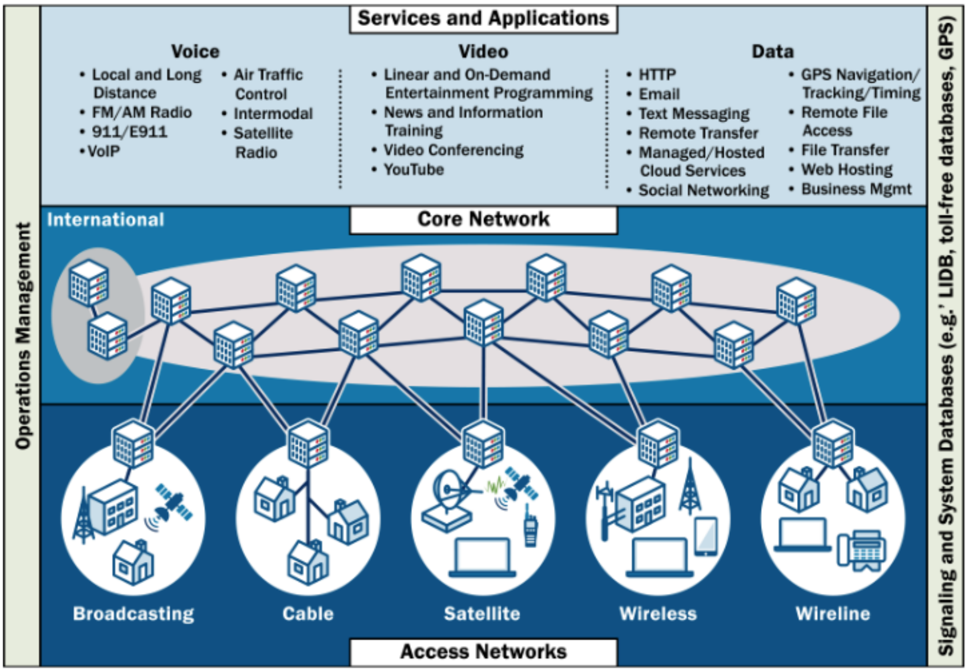


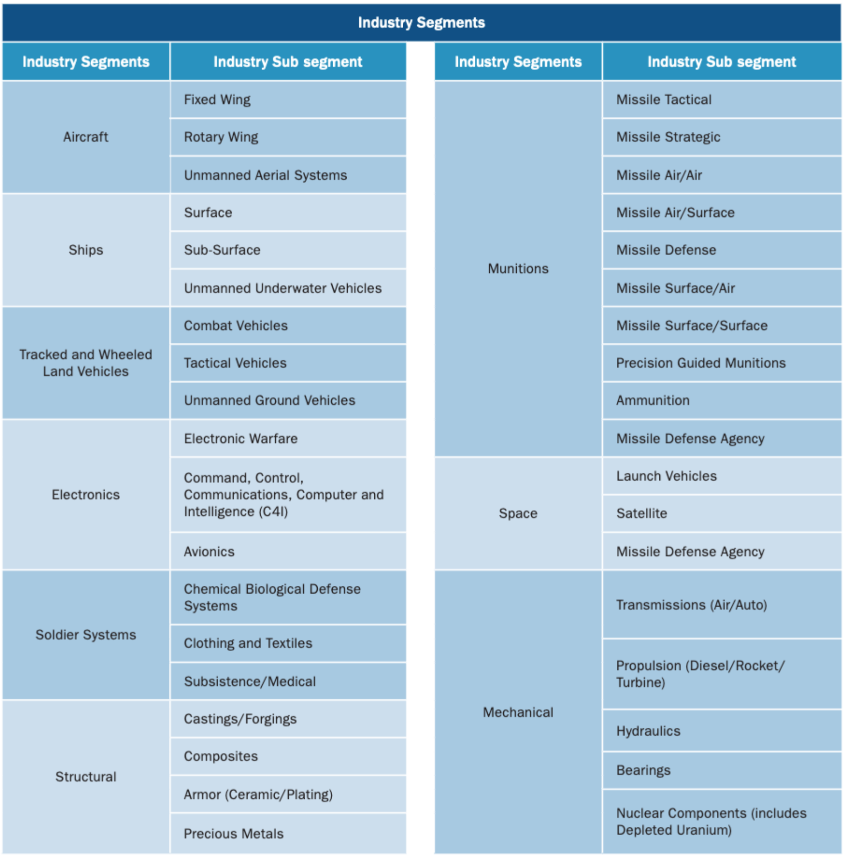
Figure 4.1: Services and Application in the Communications Sector [39]

4.2.4 Dams Sector

Providing critical water retention, hydroelectric power generation, municipal and industrial water supplies and more, the Dams Sector is crucial for creating energy and protecting population against flooding [40]. It's not obvious that satellites play a part in the operations of this sector, however, the UK Space Agency has developed a satellite system called DAMSAT to improve dam safety. DAMSAT provides monitoring through satellite images, together with weather forecasts, to spot dangerous movement and indicators of leakage. Dam-leakage and failure has proven to be lethal [41], monitoring and surveillance is therefore important to ensure residents safety. DAMSAT falls under the category of Earth Observation Satellites and is therefore interconenected to such systems.

4.2.5 Defense Industrial Base Sector

Not surprisingly, the Defense Industrial Base sector relies heavily on satellites and space systems. Éléonore Daxhelet says that space systems are an important asset for the defense sector. Satellite imagery proves crucial in military strategy and planning, providing information about actor's infrastructure and movements which helps with surveillance and intelligence gathering. They also contribute to battleground and weather conditions, enhancing mission planning [42]. Cilufo agrees to the importance of satellites in the defense sector, stating in his commending paper about approving space systems as critical infrastructure that space systems serve as the foundation for military operations, mission assurance, intelligence, surveillance, and reconnaissance [43]. This dependency is not unique for the United States. According to the UCS Satellite Database 31 different countries, including Norway (1), operate satellites with military function. The US is however the biggest operator (239), followed by China (140), Russia (105), France (18), and Italy (13). Israel and India follow with respectively 11 and 9 each [44] [20]. Already in 2001, The U.S.' recognized their dominance in space, claiming that in the context of national security; "The U.S. is more dependent on space than any other nation" [45]. CISA confirms this dependency, as seen in figure 4.2 explaining the DIB's industry segments, where space and satellites are listed as segment and sub-segment. Accordingly, the DIB sector is highly interconnected to Earth Observation through imagery satellites and GPS through vehicles, ships, and planes[46].



Industry Segments			
Industry Segments	**Industry Sub segment**	**Industry Segments**	**Industry Sub segment**
Aircraft	Fixed Wing	Munitions	Missile Tactical
	Rotary Wing		Missile Strategic
	Unmanned Aerial Systems		Missile Air/Air
Ships	Surface		Missile Air/Surface
	Sub-Surface		Missile Defense
	Unmanned Underwater Vehicles		Missile Surface/Air
Tracked and Wheeled Land Vehicles	Combat Vehicles		Missile Surface/Surface
	Tactical Vehicles		Precision Guided Munitions
	Unmanned Ground Vehicles		Ammunition
Electronics	Electronic Warfare		Missile Defense Agency
	Command, Control, Communications, Computer and Intelligence (C4I)	Space	Launch Vehicles
	Avionics		Satellite
Soldier Systems	Chemical Biological Defense Systems		Missile Defense Agency
	Clothing and Textiles	Mechanical	Transmissions (Air/Auto)
	Subsistence/Medical		Propulsion (Diesel/Rocket/ Turbine)
Structural	Castings/Forgings		Hydraulics
	Composites		Bearings
	Armor (Ceramic/Plating)		Nuclear Components (includes Depleted Uranium)
	Precious Metals		

Figure 4.2: Industry segments in the DIB sector [47]

4.2.6 Emergency Services Sector

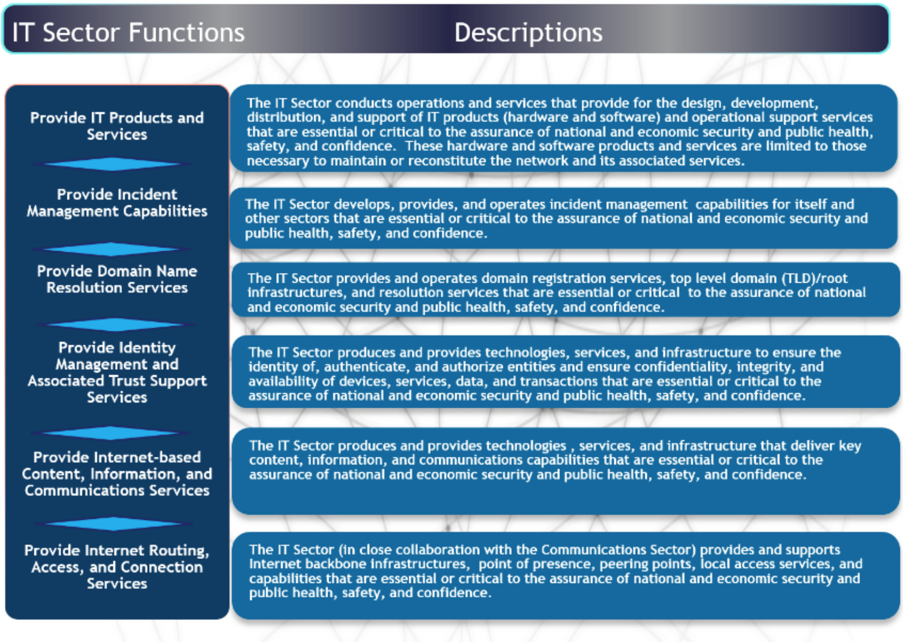
Consisting of incident response for police, medical, fire, and rescue, the Emergency Services sector is heavily dependent on the Communications sector to communicate with each other, and potential victims [48]. Following the scope, however, we need to identify direct satellite interconnections. Such direct interconnections exist through Global Positioning System (GPS), and timing (PNT) applications, which are crucial for incident response and coordination [49]. Inmarsat satellite company also argues that satellite communication is essential for disaster response, as they are easy to deploy and set up, they provide global coverage with remote site connectivity while providing reliable voice and broadband data traffic. Their independence from terrestrial infrastructure makes them ideal in case of disaster, where terrestrial infrastructure might be damaged or ruined [50] [51]. Consequently this sector is reliant on both GPS and Communication Satellites.

4.2.7 Food and Agriculture Sector

While mostly reliant on terrestrial infrastructure like transportation, energy, chemical, and water systems [52], several researchers have exclaimed the Food and Agriculture sector's utilization of satellites. Lieutenant Colonel Justin D. Ellsworth claims that; "America's farmers rely on satellite data to monitor soil, water assessments, crop developments, and much more for their livelihoods and our agricultural industry." [38]. Remote sensing, weather monitoring and forecasts also provide key data to farmers [49][53]. Georgescu acknowledges this, naming this satellite-assisted cultivation as "precision agriculture" and underlining its importance for effective crop development and management [54]. This sector's interconnection to Earth Observation satellites is therefore clear.

4.2.8 Information Tecehnology Sector

CISA defines six different functions they consider critical to provide high-assurance IT products and services. These functions can be seen in the figure below [55].



IT Sector Functions	Descriptions
Provide IT Products and Services	The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products (hardware and software) and operational support services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. These hardware and software products and services are limited to those necessary to maintain or reconstitute the network and its associated services.
Provide Incident Management Capabilities	The IT Sector develops, provides, and operates incident management capabilities for itself and other sectors that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Domain Name Resolution Services	The IT Sector provides and operates domain registration services, top level domain (TLD)/root infrastructures, and resolution services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Identity Management and Associated Trust Support Services	The IT Sector produces and provides technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet-based Content, Information, and Communications Services	The IT Sector produces and provides technologies , services, and infrastructure that deliver key content, information, and communications capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet Routing, Access, and Connection Services	The IT Sector (in close collaboration with the Communications Sector) provides and supports Internet backbone infrastructures, point of presence, peering points, local access services, and capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.

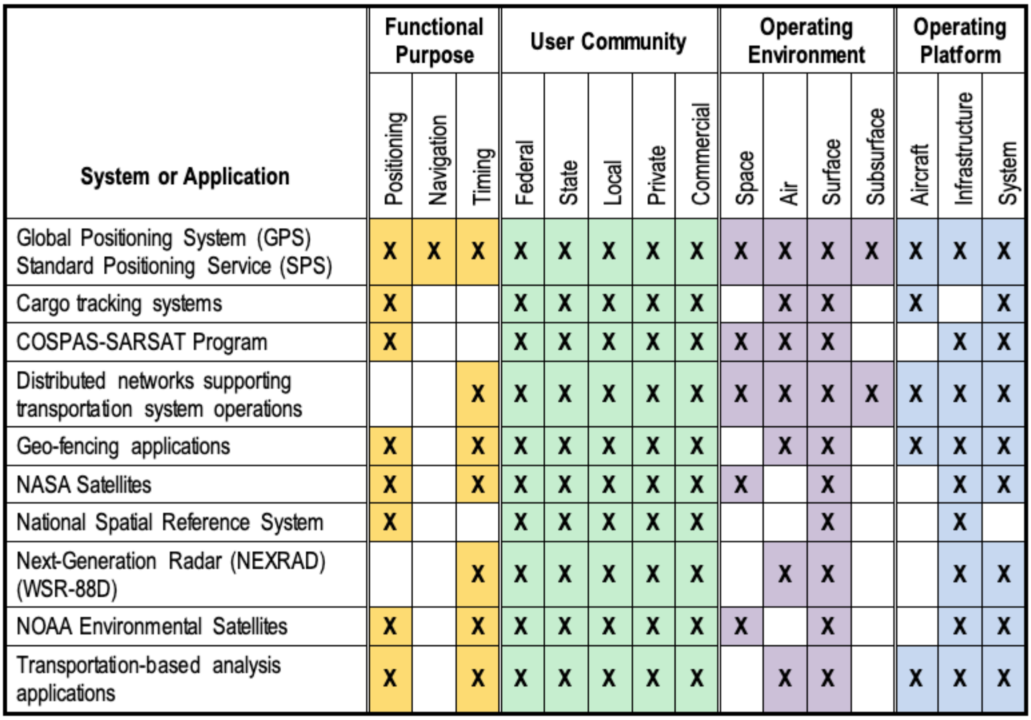
Figure 4.3: IT Sector Functions [55]

As stated in the diagram, the IT sector is responsible for providing internet backbone infrastructure, technologies, services, and infrastructure that deliver key content, information, and communications capabilities. This includes reliance on GPS, Internet, and Communications Satellites.

4.2.9 Transportation Systems Sector

GPS and Positioning, Navigation, and Timing (PNT) applications are services provided by satellites that prove crucial for the Transportation Systems sector [49]. Research shows that effective use of Global Navigation Satellite Systems (GNSS), which GPS is a subset of [56], and Intelligent Transport Systems (ITS)[57], can provide safer and greener transport [58].

Eric Wallischeck summarizes further interconnections for space, air, surface, and subsurface transportation in his paper about transportation dependencies, which can be seen in 4.4.



System or Application	Functional Purpose			User Community					Operating Environment				Operating Platform		
	Positioning	Navigation	Timing	Federal	State	Local	Private	Commercial	Space	Air	Surface	Subsurface	Aircraft	Infrastructure	System
Global Positioning System (GPS) Standard Positioning Service (SPS)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Cargo tracking systems	X			X	X	X	X	X		X	X		X		X
COSPAS-SARSAT Program	X			X	X	X	X	X	X	X	X			X	X
Distributed networks supporting transportation system operations			X	X	X	X	X	X	X	X	X	X	X	X	X
Geo-fencing applications	X		X	X	X	X	X	X		X	X		X	X	X
NASA Satellites	X		X	X	X	X	X	X	X		X			X	X
National Spatial Reference System	X			X	X	X	X	X			X			X	
Next-Generation Radar (NEXRAD) (WSR-88D)			X	X	X	X	X	X		X	X			X	X
NOAA Environmental Satellites	X		X	X	X	X	X	X	X		X			X	X
Transportation-based analysis applications	X		X	X	X	X	X	X		X	X		X	X	X

Figure 4.4: Systems and applications used in Transportation Systems [59]

Based on this information, GPS and Earth Observation (through ITS) Satellites are relevant technologies for the Transportation Systems sector.

4.2.10 Summary

Out of the 16 critical infrastructure sectors defined by CISA, direct satellite interconnections has now been identified in 9 of them. That is not to say that the remaining 7; Critical Manufacturing, Energy, Financial Services, Government Facilities, Healthcare, Nuclear reactors, and Water and Wastewater Systems, don't rely on satellites at all. However, they don't have a direct interconnection to satellites, they are rather dependent on a different sector to provide them with satellite supported infrastructure, and therefore not a part of this thesis' scope. A summary of all sectors and their respective interconnected satellite technologies is seen in table 4.1.

Sector	**Satellite Technologies**
Chermical	Earth Observation, GPS
Commercial Facilities	Broadcast
Communications	Broadcast, Communication, GPS
Dams	Earth Observation
Defense Industrial Base	Earth Observation, GPS
Emergency Services	Communication, GPS
Food and Agriculture	Earth Observation
Information Technology	Communication, GPS, Internet
Transportation Systems	Earth Observation, GPS

Table 4.1: Summary of technology interconnected to critical infrastructure sectors

Chapter 5
Attack Path Analysis Methodology

In this chapter, research and investigation to answer research question 3: "What is the most appropriate methodology to identify attack paths and assess risk?" will be conducted. The results of this research will be used in practice in Chapter 6 to identify attack paths.

5.1 Methodology

In a system of networked assets, an attack path is defined by S. Katsikas and G. Kavallieratos as "an ordered sequence of assets that can be used as stepping stones by an attacker seeking to attack one or more assets on the path." [60]

Several methods for analyzing attack paths have been proposed in the literature [61]. In [62] a method to effectively generate attack graphs through constraints and Depth-first search is proposed. This has been used to identify attack paths in the maritime domain. Further, the Adversary View Security Evaluation (ADVISE) modeling approach is proposed in [63] in order to simplify the understanding of attack paths within cyber-physical systems. Also, a set of algorithms to prioritize a system's attack paths by its vulnerabilities was proposed in [64]. Another technique to analyze attack paths in cyber physical systems based on Common Vulnerabilities and Exposures, and the Common Vulnerability Scoring System was proposed in [65].

However, to perform an attack path analysis in accordance with the research question, the "Attack Path Analysis for Cyber Physical Systems" developed by S. Katsikas and G. Kavallieratos [60] is found to be the most appropriate methodology, because it assess cyber physical systems in a general and comprehensive manner suitable for satellite systems. The methodology follows the steps depicted in 5.1 and is more thoroughly described in sector 5.2.

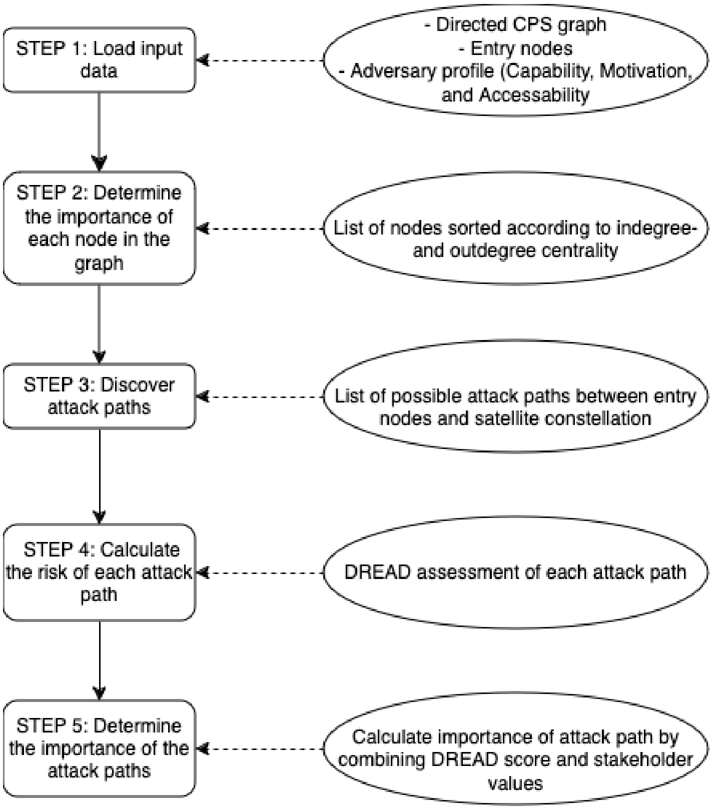

STEP 1: Load input data
- Directed CPS graph
- Entry nodes
- Adversary profile (Capability, Motivation, and Accessability
STEP 2: Determine the importance of each node in the graph
List of nodes sorted according to indegree- and outdegree centrality
STEP 3: Discover attack paths
List of possible attack paths between entry nodes and satellite constellation
STEP 4: Calculate the risk of each attack path
DREAD assessment of each attack path
STEP 5: Determine the importance of the attack paths
Calculate importance of attack path by combining DREAD score and stakeholder values

Figure 5.1: Stepwise Attack Path Methodology from [60]

5.2 Requirements

5.2.1 Input Data

The input data required to start the analysis is a directed graph *G(V,E)* visualizing the Cyber Physical System (CPS). This should include all distinct components required for the CPS to function. Entry nodes for where an adversary could start an attack also needs to be determined in this first step. The entry nodes will always contain one node from the user segment, and one node from the ground segment. The node representing the user segment will in all cases be the UT.

Further, to correctly determine the criticality of, and whether or not an attack path is feasible, an assessment of the *Accessibility, Capability,* and *Motivation* of an assumed adversary needs to be done. If an adversary doesnt meet the required levels of *Accessibility, Capability, and Motivation*, there are no feasible attack paths. The levels are determined through the following measures proposed by [60]:

- Accessibility is a measure of the adversary's logical and physical accessibility of the adversary to the attack surface of each entry sub-system. It assumes a ”yes” or ”no” value.
- Capability represents the ability of the adversary to access the necessary resources (technical, physical, and logical) to perform an attack against each entry sub-system. It is measured in a qualitative scale ranging from “Low” to “Medium” to “High”.
- Motivation represents the determination of the adversary to carry out the attack. It is measured in a qualitative scale ranging from “Low” to “Medium” to “High”.

In this thesis only one adversary will be considered when conducting the attack path analysis. This is based off the research done in [66] and [5] which states that most satellite attacks are done by state and military actors. An imaginary state actor with high levels of accessibility, capability, and motivation is therefore used as the assumed adversary.

5.2.2 Node Criticality

Contrary to the method used and developed in [60] and [67], the *Tacit Input Centrality (TIC), Tacit Output Centrality (TOC)* , and *Closeness Centrality* metrics are not used to determine the criticality of nodes, as this thesis operates with less complex graphs. The main component in the CPSs investigated in this thesis will always be the Satellite constellations, because they are the hardware needed to provide information and data to UTs. This node is therefore considered the most critical in every CPS. The remaining nodes are then ranked by their node indegree and outdegree centrality, which indicate the number of links entering and leaving a node. This is used as a metric because those nodes with high indegree and outdegree are considered important. Bidirectional arrows entering and leaving nodes count 2 points.

5.2.3 Attack Paths

The possible attack paths between the entry node and target node in the directed graph is discovered by performing a depth-first search including all non-circular paths [60].

5.2.4 Attack Path Risk

Next, the risk associated with each critical CPS component must be estimated. Katsikas and Kavallieratos recommend using the Microsoft-developed *DREAD* method which provides a quantitative estimate of software systems risk. DREAD stands for

Damage, Reproducibility, Exploitability, Affected users/systems, and Discoverability. Each of these factors receives an integer score from 0 to 3, assessed by a set of criteria which can be seen in table 5.1.

	High (3)	**Medium (2)**	**Low (1)**
D	The adversary is able to bypass security mechanisms; get administrator access; upload/modify the CPS content	Leakage of confidential information of the CPS (functions/source code); inflict partial malfunction/disruption to the system	Leaking non-sensitive information; the attack is not possible to be extended over other CPSs
R	The cyberattack can be reproduced anytime to the targeted CPS	The adversary is able to reproduce the attack but under specific risk conditions	Although they know CPS's vulnerabilities/faults, the attacker is not able to perform the cyberattack
E	The cyberattack can be performed by a novice adversary in a short time	A skilled adversary could launch the attack	The attack requires an extremely skilled person and in-depth knowledge of the targeted CPS
A	All CPSs are affected	Partial users/systems, non-default configuration	The attack affects only the targeted CPS
D	The CPS's vulnerabilities are well known and the attacker is able to get access to the relevant information to exploit the vulnerabilities	The CPS's vulnerabilities/faults are not well known and the adversary needs to get access to the CPS	The threat has been identified and the vulnerabilities have been patched

Table 5.1: DREAD Criteria composed by [60]

A DREAD score is then calculated with values derived from table 5.1 accordingly:

$$\frac{\sum(Damage, AffectedSystems)}{2} = Impact \tag{5.1}$$

$$\frac{\sum(Reproducibility, Exploitability, Discoverability)}{3} = Likelihood \tag{5.2}$$

$$DREADscore = \frac{(Impact + Likelihood)}{2} \tag{5.3}$$

The total DREAD risk level is then derived from the following criteria [60]:

If *DREAD score* ≤ 1 **then** *DREAD risk level* := LOW

If $1 <$ *DREAD score* ≤ 2 **then** *DREAD risk level* := MEDIUM

If $2 <$ *DREAD score* ≤ 3 **then** *DREAD risk level* := HIGH

5.2.5 Attack Path Importance

The last step in the analysis is to determine the importance of the whole attack path. To do this, the stakeholder of the system assess the importance of each node with the *CPSImp* metric. The CPSImp is assigned to each node in the system by a relevant stakeholder and can take one of the following values [60]:

- (1): Low importance (potential system damage or disruption cannot inflict any significant damage to the overall system);
- (2): Medium importance (if the system is damaged or disrupted, overall system malfunctions may occur, but no crucial deviation from normal operation);
- (3): High importance (if the system is damaged or disrupted, the operation of the overall system will be severely affected)

The importance of a discovered attack path is then determined considering both the DREAD risk level and the CPSImp calculated with equation (6.4)

$$AttackPathImportance = 0.6 * CPSImp + 0.4 * DREADrisk \tag{5.4}$$

Chapter 6
Attack Path Analysis

After describing the methodology for conducting an attack path analysis for a CPS in chapter 5, this chapter will provide the analysis in its entirety using said methodology. This is in order to answer research question 4.

6.1 General Satellite Systems

Before introducing each distinct satellite service identified in chapter 4, it is important to understand the basic composition of a space system. Space systems consist of mainly four segments; space, link, ground, and user, as shown in figure 6.1 [68]. The space segment is where satellites are located, but it also includes probes, capsules, space telescopes, and space shuttles. Interconnections of centers, stations, and spacecraft with ground and space communication links define the link segment, while the ground segment includes the ground-based infrastructure, services, support mechanisms, and personnel to operate and control the space systems. At last, the user segment consists of the services provided to end-users by the space infrastructure. This can be internet connection, GPS, and TV broadcasts [68].

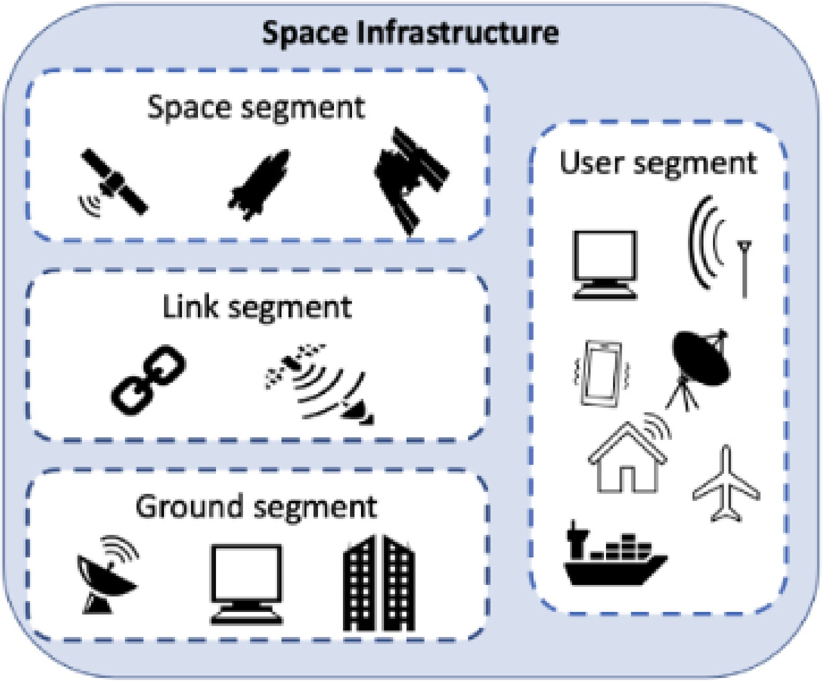


Figure 6.1: Space Infrastructure Segments [68]

6.2 GPS and PNT

6.2.1 Input Data

Step 1 involves determining the input data for the analysis. This includes the directed graph in 7.1, the assumed adversary described in 6.2.1, and the targeted node, which in this case is the "GPS Satellite Constellation". As discussed, the entry nodes for this attack path analysis are one from the user segment and one from the ground segment. Respectively, the User Terminals and Master Control Station nodes are chosen.

In the space segment, GPS is operated by 31 medium Earth orbit (MEO) satellites, where each satellite circles the Earth twice a day transmitting radio signals to users. The GPS constellations currently exist of 6 legacy satellites and 25 modernized satellites [69].

The control/ground segment consists of three distinct elements; the master control station, monitor stations, and ground antennas scattered across the globe.

Providing command and control of the GPS constellation is the master control station. Acting like a singular system brain, this element computes the precise locations of all satellites, generates navigation messages, and monitors satellite broadcasts to ensure constellation health and accuracy. The master control station is significantly important and is therefore backed up by a fully operational and redundant alternate master control station [70]. Monitor stations provide global coverage via 16 sites around the globe. They are responsible for tracking the GPS satellites and collecting navigation signals, range/carrier measurements and atmospheric data, which are then fed to the master control station. The last element of the ground segment is the 11 ground antennas, which send commands, navigation data uploads, and receive telemetry. These antennas communicate via S-band and perform S-band ranging to provide anomaly resolution and early orbit support [70].

The US government describes GPS as an essential element of the global information infrastructure, as the free and open nature of GPS has led to the development of applications and services that are used in agriculture, transportation, information technology, and communication. In other words, the user segment of the GPS constellation is the part that interacts with ordinary people through applications and services [71]. A node representation of the GPS constellation is depicted in figure 6.2.

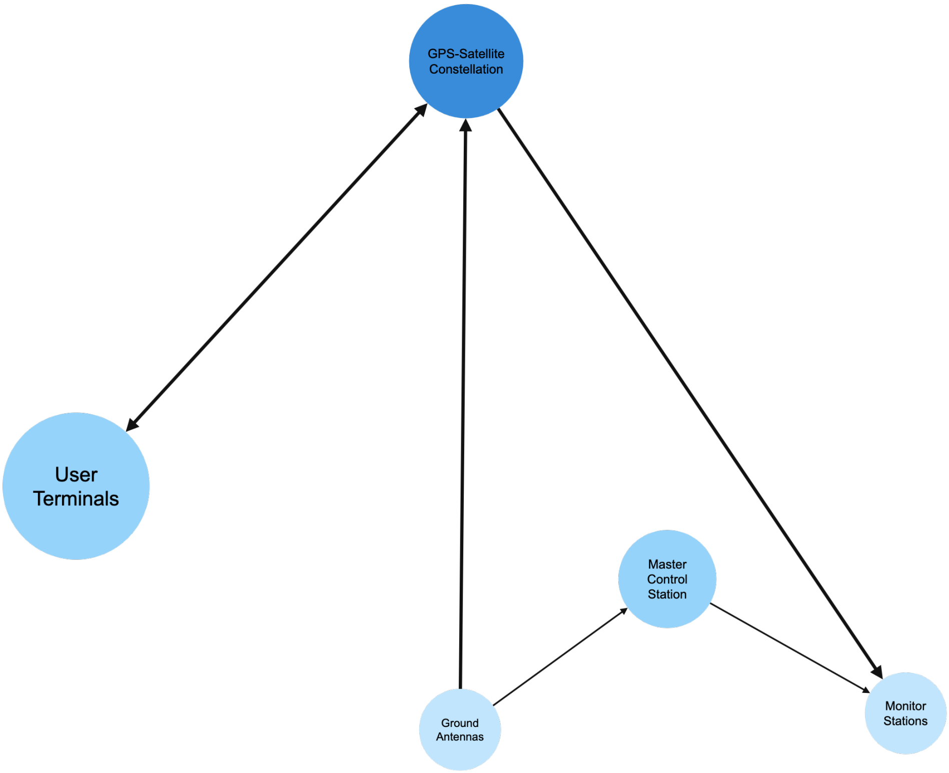


Figure 6.2: GPS CPS represented by a directed graph

6.2.2 Node Criticality

The importance of the nodes in graph 6.2 is assessed according to the method described in 5.2.2, and the result is seen in table 6.1

Node	**Indegree + Outdegree Centrality**
GPS-Satellite Constellation	4
Master Control Station	2
Ground Antennas	2
Monitor Stations	2
User Terminals	2

Table 6.1: GPS Node Criticality

6.2.3 Attack Paths

Feasible attack paths are determined by discovering all possible paths from the entry points to the target GPS-Satellite Constellation node. Possible paths are displayed in the following two tables, where table 6.2 represents all available paths with entry points from the user segment, and table 6.3 shows the available paths when the entry point is in the ground segment.

Path ID	**UT - GPS Satellite**
GPS_1	UT - GPS

Table 6.2: Attack Paths from UT to GPS Satellites

Path ID	**GA - GPS Satellite**
GPS_2	GA - GPS
GPS_3	GA - MCS - MS - GPS

Table 6.3: Attack Paths from GA to GPS Satellites

6.2.4 Attack Path Risk

The risk of each node traversed in the attack paths in table 6.2 and 6.3 are assessed with the DREAD method, as described in 5.2.4.

First considering the space segment consisting of 31 MEO satellites:

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R	X		
E			X
A	X		
D		X	

Table 6.4: Satellites in GPS

As derived from [69] it is known that the constellation of 31 MEO satellites is interconnected and therefore a possibility to disrupt one satellite, may lead to disruption of several satellites through the Inter Satellite Links (ISLs). However, administrator access is not possible to get without going through the Master Control Station, so D=2. Because several of the constellation's satellites are legacy satellites with old software, and software with bugs in existing satellites is found hard to update R is given score 3. As discussed in section 5.2.1 the adversaries that poses a threat to satellite systems are highly sophisticated, therefore the E is set to 1.

Because the satellites in a GPS constellation are connected to both the user and control/ground segment, these CPSs may also be affected by a rogue satellite providing false data, a High (3) score is therefore given. As seen earlier in this thesis most satellite infrastructure practice "security through obscurity", this corresponds to the Medium (2) score.

Using the equations in section 5.2.4 this results in a DREAD risk level $High = 2{,}75$ for the GPS satellite constellation.

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.5: Monitor Stations

Since monitor stations are physical hardware communicating with the Master Control Station and the satellites, an adversary that can gain physical access to this station will be able to modify the communication sent between this CPS and the Master Control Station. The leakage of confidential information can lead to this, and a D = 2 is therefore given. This attack may however be hard to reproduce as physical access to the station might be required, consequently R = 2.

To conduct an attack knowledge about the location of Monitor Stations and competence to hijack the communication channel between Monitor and Master Control stations is required. Such an adversary is highly skilled and consequently E = 1.

An attack against a monitor station will affect the data given to the Master Control Station and therefore impact the whole system. However, it does not have the same direct impact as an attack against the Master Control Station, hence A = 2. The vulnerabilities present in a Monitor Station are not well known and would require access to the physical element to do substantial damage, so D = 2. This DREAD matrix results in a *High* = 2,25 DREAD risk level.

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.6: Ground Antennas

Since Ground Antennas serve approximately the same purpose as Monitor Stations and have almost the same properties, its DREAD matrix is identical to Monitor Stations'. Similarly, it has a *High* = 2,25 DREAD risk level.

	High (3)	**Medium (2)**	**Low (1)**
D	X		
R		X	
E			X
A	X		
D		X	

Table 6.7: Master Control Station

Acting like the brain of the whole GPS constellation, access, and control of a Master Control Station can provide administrator access to the whole system. Hence, the score D = 2 is given. Like the Monitor Station, physical access to the MCS is required to cause significant damage. Such access might be hard to reproduce and therefore R = 2. Again, adversaries conducting an attack of this magnitude would be highly skilled, hence E = 1.

An attack against the Master Control Station affects all components of the GPS system, because the MCS is the brain behind the system. Therefore A = 3. As mentioned, substantial damage can only be inflicted with physical access, so D = 2. This gives a *High* = 2,75 DREAD risk level.

	High (3)	**Medium (2)**	**Low (1)**
D			X
R		X	
E		X	
A			X
D		X	

Table 6.8: User Terminals

Because UTs are somewhat disconnected from the rest of the CPS it would be hard for the adversaries to extend the attack to other nodes from the UT. Further, UTs are given Low or Medium scores in every category because of its independence in the CPS. The above matrix results in a *Medium* = 2 DREAD risk level.

6.2.5 Attack Path Importance

Including the risk and the CPSImp, the importance of each attack path is calculated with the equation in 5.2.5 and shown in table 6.9. From table 6.10 it's clear that GPS_3 is the most critical path.

Node	**CPSImp**
GPS-Satellite Constellation	3
Master Control Station	3
Ground Antennas	2
Monitor Stations	2
User Terminals	1

Table 6.9: GPS CPSImp

Path ID	Affected CPSs	Attack Path Importance
GPS_3	GA - MCS - MS - GPS	10
GPS_2	GA - GPS	5
GPS_1	UT - GPS	4,3

Table 6.10: Attack Paths ranking

6.3 Communication Satellites

Using the same methodology and approach as in 6.2 the analysis for Satellite Communication is conducted.

6.3.1 Input Data

Similar to the GPS architecture, satellite communication services are divided into space, control, and user segments.

In this case, the space segment consists of low Earth orbit (LEO), satellite constellations connected by ISLs carrying so-called Onboard Processing (OBP) payloads. The satellites connect to the ground segment's gateways through feeder links. Gateways consist of antennas, baseband processing units, routers, and core network entities. Governing the gateways is the NMC, it routes internet traffic and manages the network. The user segment contains various mobile and fixed User Terminals, however, the satellites don't need to send signals via gateways to reach the UTs. This is because the OBP payloads enable satellites to directly provide radio access to users through Medium Access Control (MAC) and Radio Link Control (RLC) protocols, acting like a space base station [72]. A node representation of the Communication Satellite system is shown in 6.3.

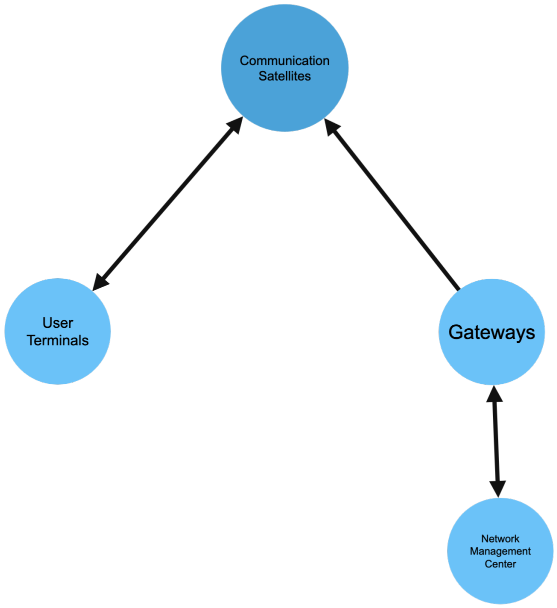


Figure 6.3: Node representation of the Communication Satellite system

6.3.2 Node Criticality

Again, the existent nodes in the Communication Satellite system are sorted by their criticality in table 6.11.

Node	Indegree + Outdegree Centrality
Communication Satellites	3
Gateways	3
Network Management Center	2
User Terminals	2

Table 6.11: Communication Node Criticality

6.3.3 Attack Paths

Available attack paths are shown in the subsequent tables, where respectively UTs and Network Management Center are used as adversary entry points.

Path ID	UT - Communication Satellites
Comm.Sat_1	UT - Comm.Sat

Table 6.12: Attack Paths from UT to Communication Satellites

Path ID	NMC - Communication Satellites
Comm.Sat_2	NMC - Gateway - Comm.Sat

Table 6.13: Attack Paths from NMC to Communication Satellites

6.3.4 Attack Path Risk

All the nodes present in Communication Satellite CPS has a resemblance to the nodes in the GPS CPS. Thus, similar DREAD scores are given to these respective nodes. This includes the Communication Satellites, which are like the GPS satellites, Gateways which are similar to Monitor Stations and Ground Antennas, the NMC with same functionality as the MCS, and of course the UTs.

	High (3)	Medium (2)	Low (1)
D		X	
R	X		
E			X
A	X		
D		X	

Table 6.14: Communication Satellites

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.15: Gateways

	High (3)	**Medium (2)**	**Low (1)**
D	X		
R		X	
E			X
A	X		
D		X	

Table 6.16: Network Management Center

	High (3)	**Medium (2)**	**Low (1)**
D			X
R		X	
E		X	
A			X
D		X	

Table 6.17: User Terminals

6.3.5 Attack Path Importance

After assigning each node with a CPSImp value and calculating the attack path importance, it’s clear that *Comm.Sat_2* is the most substantial and critical path.

Node	**CPSImp**
Communication Satellite Constellation	3
Network Management Center	2
Gateways	2
User Terminals	1

Table 6.18: Communication Satellites CPSImp

Path ID	Affected CPSs	Attack Path Importance
Comm.Sat_2	NMC - Gateway - Comm.Sat	7.3
Comm.Sat_1	UT - Comm.Sat	4,3

Table 6.19: Attack Paths ranking for Communication Satellites

6.4 Broadcast Satellites

6.4.1 Input Data

For the case of Broadcast Satellites, a specific broadcasting system called Sirius XM Radio is used as a reference architecture. Sirius XM Radio broadcasts continuous high-quality audio, video and data content while also being a primary entry point for the Emergency Alert System (EAS) [73]. It consists of Sirius satellites and a VSAT satellite in the space segment. The Sirius satellites broadcast audio and data signals to UTs through time-division multiplexing (TDM), while the VSAT transmits the same signal to an array of terrestrial repeaters which again transmits to the same UTs, providing redundancy and gap-filling coverage. Also, a part of the ground segment is a remote uplink site and a studio, which generates the audio and video content. The studio broadcasts the content to the remote uplink site, which then sends the signal to the Sirius satellites. It also sends the content directly to the VSAT to provide redundancy. The whole architecture can be seen in figure 6.4 [74].

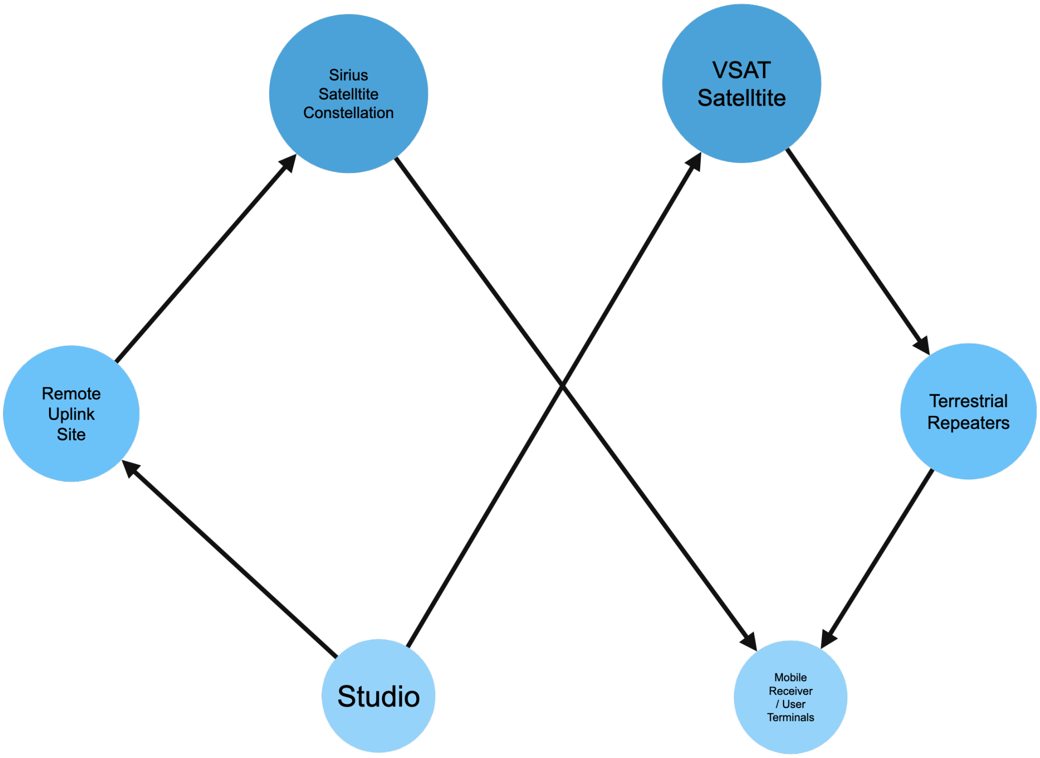


Figure 6.4: Node representation of Broadcast Satellite system

6.4.2 Node Criticality

Node	Indegree + Outdegree Centrality
Sirius Satellite Constellation	2
VSAT satellite	2
Remote Uplink Site	2
Terrestrial Repeaters	2
Studio	2
User Terminals	2

Table 6.20: Broadcast Satellite Node Criticality

6.4.3 Attack Paths

Because the Sirius XM architecture involves two distinct satellite constellations, Sirius satellites and VSAT, both are considered as target nodes. The entry node is in both cases the Studio, since this is the only node that can reach both targets.

Path ID	Studio - Sirius Satellites
Broadcast_1	Studio - RUS - Sirius Satellite Constellation

Table 6.21: Attack Paths from Studio to Sirius Satellites

Path ID	Studio - VSAT
Broadcast_2	Studio - VSAT

Table 6.22: Attack Paths from Studio to VSAT

6.4.4 Attack Path Risk

Similar to the GPS and Communication, the Sirius Satellite Constellation receives the same DREAD matrix. The VSAT satellite however is not as critical as Sirius, because it acts more like a redundancy. It therefore receives a lower DREAD risk level equivalent to the Remote Uplink Site and Studio, which has the same attributes as the Ground Antennas in GPS.

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R	X		
E			X
A	X		
D		X	

Table 6.23: Sirius Satellite Constellation

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.24: VSAT Satellite

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.25: Remote Uplink Site

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.26: Studio

6.4.5 Attack Path Importance

Once again, the path including the most nodes is the most critical. For Broadcasting Satellites this is the *Broadcast_1* path.

Node	**CPSImp**
Sirius Satellite Constellation	3
VSAT Satellite	2
Remote Uplink Site	2
Studio	2

Table 6.27: Broadcast Satellites CPSImp

Path ID	**Affected CPSs**	**Attack Path Importance**
Broadcast_1	Studio - RUS - Sirius Satellite Constellation	7.1
Broadcast_2	Studio - VSAT	4,2

Table 6.28: Attack Paths ranking for Broadcast Satellites

6.5 Satellite Internet

6.5.1 Input Data

To further investigate the architecture behind satellite internet SpaceX's Starlink which was initially mentioned in the background section of this thesis, is used as an example. Claimed to be the world's most advanced broadband satellite internet [75], the Starlink constellation consists of thousands of LEO satellites packed with cutting edge technology. The Starlink satellites utilize optical space-lasers as ISLs to communicate and send data between satellites. At the ground, different gateways and stations are located around the world providing internet connectivity to the satellites. These stations are connected to an Internet Service Provider (ISP)via fiber. Internet is provided to UTs in the user segment through a Starlink Dish Antenna which is again connected to a Starlink Wi-Fi router. A visualization of this architecture can be seen in figure 6.5 [76] [77].

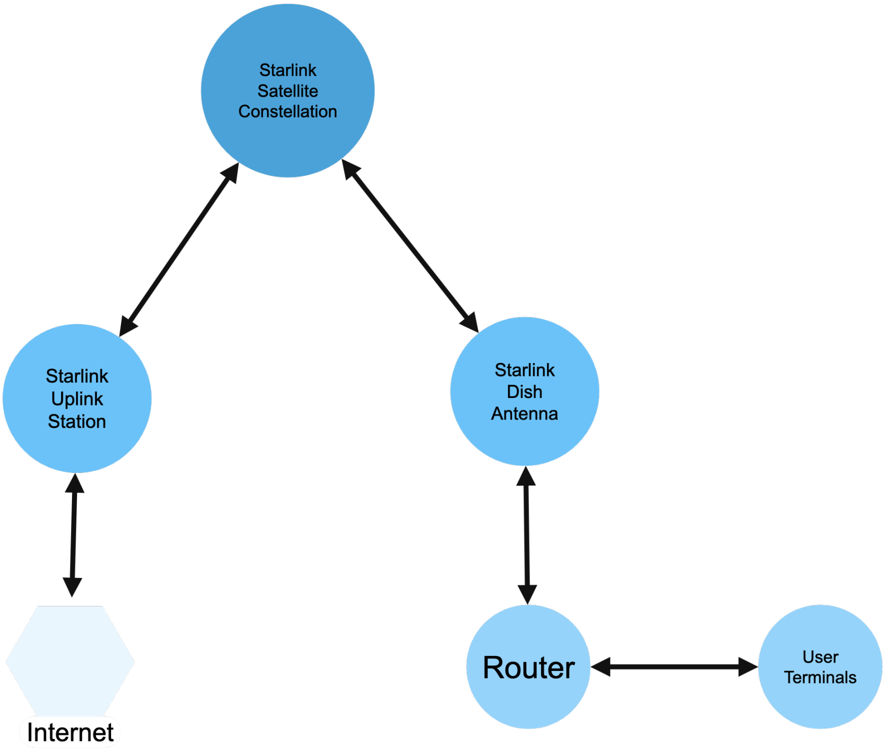


Figure 6.5: Node representation of the Starlink Satellite system

6.5.2 Node Criticality

Node	Indegree + Outdegree Centrality
Starlink Satellite Constellation	4
Starlink Uplink Station	4
Starlink Dish Antenna	4
Router	4
User Terminals	2

Table 6.29: Starlink Node Criticality

6.5.3 Attack Paths

Regarding the Starlink Satellite system, the Starlink Uplink Station and User Terminals are considered as the two entry nodes.

Path ID	SUS - Starlink
Starlink_1	SUS - Starlink

Table 6.30: Attack Paths from Starlink Uplink Station to Starlink Satellites

Path ID	UT - Starlink
Starlink_2	UT - Router - SDA - Starlink

Table 6.31: Attack Paths from User Terminals to Starlink Satellites

6.5.4 Attack Path Risk

Similar to the previous CPSs' the nodes in Starlink bears resemblance to nodes in the other services. Here the SUS, SDA, and Starlink Router has the same attributes as Ground Antennas and Monitor Stations in GPS, while the Starlink Satellite Constellation undoubtedly faces the same threats as the GPS satellites.

	High (3)	Medium (2)	Low (1)
D		X	
R	X		
E			X
A	X		
D		X	

Table 6.32: Starlink Satellite Constellation

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.33: Starlink Uplink Station

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.34: Starlink Dish Antenna

	High (3)	**Medium (2)**	**Low (1)**
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.35: Starlink Router

	High (3)	**Medium (2)**	**Low (1)**
D			X
R		X	
E		X	
A			X
D		X	

Table 6.36: User Terminals

6.5.5 Attack Path Importance

Differentiating from the other systems, the Starlink Satellite system's most critical path starts with UT as entry node. This is because a signal from a UT needs to pass through two different nodes before it reaches the Starlink Satellite, while the other systems analyzed often has a direct link between UT and Satellite.

Node	**CPSImp**
Starlink	3
Router	2
Starlink Dish Antenna	2
Starlink Uplink Station	2
User Terminal	1

Table 6.37: Starlink Satellite CPSImp

Path ID	**Affected CPSs**	**Attack Path Importance**
Starlink_2	UT - Router - SDA - Starlink	8,5
Starlink_1	SUS - Starlink	5

Table 6.38: Attack Paths ranking for Satellite Internet

6.6 Earth Observation Satellites

6.6.1 Input Data

Earth Observation (EO) satellites are as the name implies satellites that surveil the Earth from outer space. In [78] it is said that Earth Observation provides an effective way of exploring the physical, chemical, and biological information related to Earth. This is done through constant and real-time monitoring of the Earth's land, ocean, atmosphere, cryosphere, and carbon cycle. Of the previously discussed services, EO satellites provide satellite imagery, surveillance, traffic data, and weather forecasting. A small real-time interactive EO satellite system consists of four elements, a User Observation Center (UOC), Ground Station (GS), Relay Satellite (RS), and an Observational Spacecraft (OS) [79]. This architecture is represented by the directed graph in 6.6.

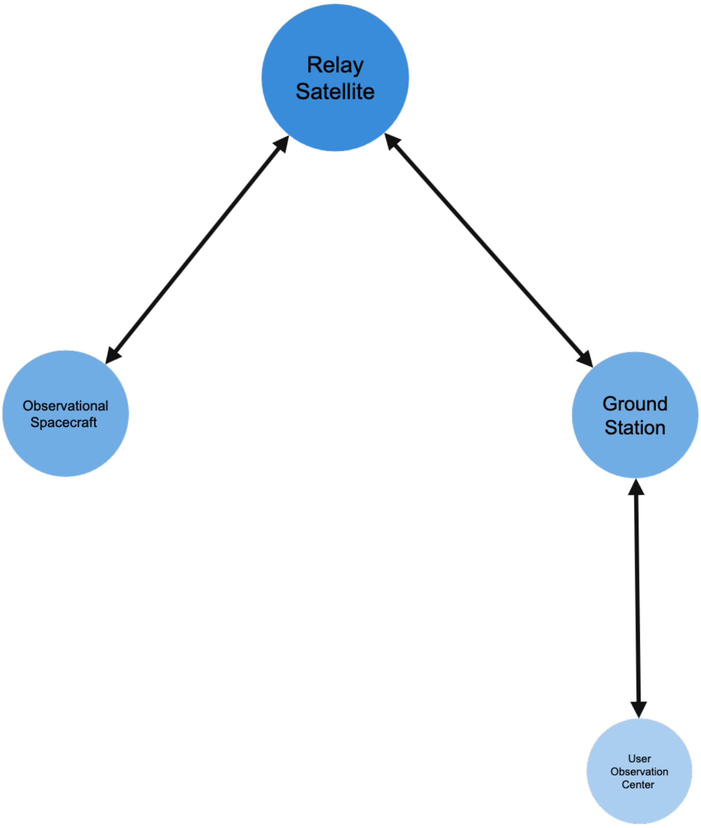


Figure 6.6: Node representation of the Earth Observation Satellite system

6.6.2 Node Criticality

Node	Indegree + Outdegree Centrality
Relay Satellite	4
Ground Station	4
User Observation Center	2
Observational Spacecraft	2

Table 6.39: Earth Observation Node Criticality

6.6.3 Attack Paths

The EO system in focus does not directly involve UTs in its architecture. It does however involve two distinct space systems, but as the focus of this thesis is to examine attack paths related to satellites, only the Relay Satellite are considered as a target node. Respectively, the UOC becomes the entry node. Only one available path exists from the UOC to the Relay Satellite as seen in table 6.40.

Path ID	UOC - Relay Satellite
EO_2	UOC - GS - RS

Table 6.40: Attack Paths from User Observation Center to Relay Satellite

6.6.4 Attack Path Risk

Also the EO CPS has similarities to previously analyzed CPSs' and the DREAD matrices are given accordingly.

	High (3)	Medium (2)	Low (1)
D		X	
R	X		
E			X
A	X		
D		X	

Table 6.41: Relay Satellite

	High (3)	Medium (2)	Low (1)
D		X	
R		X	
E			X
A		X	
D		X	

Table 6.42: Ground Station

	High (3)	Medium (2)	Low (1)
D	X		
R		X	
E			X
A	X		
D		X	

Table 6.43: User Observation Center

6.6.5 Attack Path Importance

Only one possible path exists, however it has a relatively high importance score (7,3) compared to the other paths examined earlier in this chapter.

Node	CPSImp
Relay Satellite	3
Ground Station	2
User Observation Center	2

Table 6.44: Earth Observation CPSImp

Path ID	Affected CPSs	Attack Path Importance
EO_1	UOC - GS - RS	7,3

Table 6.45: Attack Paths ranking for Earth Observation Satellites

6.7 Results

Collectively speaking, not much redundancy is present in the analyzed CPSs'. Meaning that oftentimes there only exists one distinct path from the entry node to the target node. This increases the consequence of a single link failure on this path which can cause the whole CPS to malfunction. Of the Satellite Services analyzed, only the Broadcast Satellite CPS provides some sort of redundancy through the extra VSAT satellite.

Another common trend is that the most critical paths originate in the ground segment of the space system, rather than the user segment. This may be because UTs are often just one hop away from the satellite constellations, resulting in fewer nodes being affected in a potential attack. Additionally, UTs are not integral to the operational practices of the assessed CPSs, and therefore, they are understandably not as critical in an attack path.

As shown in chapter 4 table 4.1 several of the critical infrastructure sectors have interconnections to the 5 different satellite services analyzed in this chapter. To further depict the connections between attack paths and critical infrastructure, table 6.46 shows every previously analyzed attack path with its correlating infrastructure sector. The instances in the table are sorted by the attack path criticality.

Path ID	**Affected Critical Infrastructure Sector**	**Attack Path Criticality**
GPS_3	Chemical, Communications, Defense Industrial Base, Emergency Services, Information Technology, Transportation Systems	10
Starlink_2	Information Technology	8,5
EO_1	Chemical, Dams, Defense Industrial Base, Food and Agriculture, Transportation Systems	7,3
Comm.Sat_1	Communications, Emergency Services, Information Technology	7,3
Broadcast_1	Commercial Facilities, Communications	7,1
GPS_2	Chemical, Communications, Defense Industrial Base, Emergency Services, Information Technology, Transportation Systems	5
Starlink_1	Information Technology	5
GPS_1	Chemical, Communications, Defense Industrial Base, Emergency Services, Information Technology, Transportation Systems	4,3
Comm.Sat_2	Communications, Emergency Services, Information Technology	4,3
Broadcast_2	Commercial Facilities, Communications	4,2

Table 6.46: Overview of Critical Infrastructure Sectors affected by specific attack paths

From the table it's clear that disruption or breaches in several defined paths would affect multiple critical infrastructure sectors. Especially crucial are the paths with high attack path criticality, and many affected sectors. This applies for GPS_3, EO_1, and Comm.Sat_1. This further illustrates the importance of functional and operational satellite services to keep critical infrastructure intact and operative.

A disruption in the GPS satellite system would affect several critical infrastructures and leave them with no form of navigation or positioning services. This would be especially critical for the Emergency Services, Defense, and Transportation sectors, as they rely heavily on GPS to navigate to their respective destinations. Such a disruption could in the worst-case scenario result in death if an ambulance or police car can't find their patient or victim.

Satellite Internet, however, is not directly life-threatening in case of disruption. Nevertheless, the Information Technology sector, which is interconnected to Satellite Internet, is a complex sector that provides services to other critical infrastructure sectors. Therefore, disturbance in the Information Technology sector would have repercussions for other sectors as well.

Communication and Broadcast services are also crucial for the operation of several sectors. Similar to GPS, a defective communication or broadcast system could potentially be very dangerous in a rescue operation.

Earth Observation is an important tool for monitoring weather and climate, but also for supplying the defense sector with surveillance and observation of enemies. A disruption to EO systems might not be as urgent as for GPS, but it will definitely cause a huge impact on its interconnected infrastructure.

In summary, the interconnections between critical infrastructure and satellite systems are considered to be highly relevant, and an attack against any of these satellite systems is deemed possible (through the attack path analysis) and would have a harmful effect.

Chapter 7
Mitigating Risks

This chapter aims to solve the final research question. This involves finding applicable mitigation techniques and controls to elevate the cybersecurity in the discussed satellite systems.

7.1 Mitigation Framework

Inspiration is taken from [80] to discover applicable and relevant mitigation techniques. This involves choosing the correct cybersecurity controls from a relevant framework. In this thesis the NIST SP 800-82r3 – *Guide to Operational Technology (OT) Security* is considered [81].

Out of the assessed frameworks [82] [83], NIST SP is considered the most suitable framework with viable mitigation techniques. The existing frameworks and controls in the satellite cybersecurity domain are scarce, and the ones currently available are not especially renowned. Consequently, the proposed mitigation techniques in this thesis are based on a framework that is not tailored for satellite cybersecurity, but rather more generally, Operational Technology. Satellite systems are arguably a form of OT, and the controls present in NIST SP 800-82r3 apply to the satellite systems discussed in this thesis. Benefitting from its acknowledgement and recognition in the cybersecurity field, the NIST framework is chosen to not introduce further obscurity to an already obscure domain.

Control	**Abbreviation**
Access Control	AC
Awareness and Training	AT
Auditing and Accountability	AU
Assessment, Authorization, and Monitoring	CA
Configuration Management	CM
Contingency Planning	CP
Identification and Authentication	IA
Incident Response	IR
Maintenance	MA
Media Protection	MP
Physical and Environmental Protection	PE
Planning	PL
Organization Wide Information Security Program Management Controls	PM
Personell Security	PS
Risk Assessment	RA
System and Services Acquisition	SA
System and Communications Protection	SC
System and Information Integrity	SI
Supply Chain Risk Management	SR

Table 7.1: NIST Controls derived from [81]

7.2 Mitigation Controls

Recommended controls are proposed for each threat described in DREAD and for each component the CPS' discussed in chapter 6. The results of this assessment can be seen in tables 7.2, 7.3, 7.4, 7.5, and 7.6

Component	**DREAD**	**Controls**
GPS Satellite Constellation	Damage	CA, IA, AC, SI
Master Control Station		AC, IA, AT, IA, PS, SI, SC, PM
Monitor Station		PE, AC, SI, SC
Ground Antennas		PE, AC, SI, SC
User Terminals		SC, CM, SR, SI
GPS Satellite Constellation	Reproducibility	MA, AC, CM
Master Control Station		IR, MA, AC, AT, PE, PS, SC, PM
Monitor Station		MA, PE, SC
Ground Antennas		MA, PE, SC
User Terminals		SC, MA, CM
GPS Satellite Constellation	Exploitability	SC, CA, AC, CM
Master Control Station		AT, AC, IA, PM, RA
Monitor Station		SC, CA, CM, PE
Ground Antennas		SC, CA, CM, PE
User Terminals		SC
GPS Satellite Constellation	Affected systems	CA, IA, AC, SI
Master Control Station		CA, AC, PM, SR
Monitor Station		CA, AC, PM, SR
Ground Antennas		CA, AC, PM, SR
User Terminals		SI
GPS Satellite Constellation	Discoverability	AU, MP, MA
Master Control Station		AU, MP, MA
Monitor Station		AU, MP, MA
Ground Antennas		AU, MP, MA
User Terminals		MP

Table 7.2: GPS Mitigation Controls

Component	DREAD	Controls
Communication Satellites Gateways Network Management Center User Terminals	Damage	CA, IA, AC, SI PE, AC, SI, SC AC, IA, AT, IA, PS, SI, SC, PM SC, CM, SR, SI
Communication Satellites Gateways Network Management Center User Terminals	Reproducibility	MA, AC, CM MA, PE, SC IR, MA, AC, AT, PE, PS, SC, PM SC, MA, CM
Communication Satellites Gateways Network Management Center User Terminals	Exploitability	SC, CA, AC, CM SC, CA, CM, PE AT, AC, IA, PM, RA SC
Communication Satellits Gateways Network Management Center Gateways User Terminals	Affected systems	CA, IA, AC, SI CA, AC, PM, SR CA, AC, PM, SR CA, AC, PM, SR SI
Communication Satellites Gateways Network Management Center User Terminals	Discoverability	AU, MP, MA AU, MP, MA AU, MP, MA MP

Table 7.3: Communication Satellite Mitigation Controls

Component	**DREAD**	**Controls**
Sirius Satellite Constellation	Damage	CA, IA, AC, SI
VSAT		CA, IA, AC, SI
Remote Uplink Site		AC, IA, AT, IA, PS, SI, SC, PM
Terrestrial Repeaters		PE, AC, SI, SC
Studio		AC, AT, PE, PM, PS
Mobile Receivers		SC, CM, SR, SI
Sirius Satellite Constellation	Reproducibility	MA, AC, CM
VSAT		MA, AC, CM
Remote Uplink Site		IR, MA, AC, AT, PE, PS, SC, PM
Terrestrial Repeaters		MA, PE, SC
Studio		PM
Mobile Receivers		SC
Sirius Satellite Constellation	Exploitability	SC, CA, AC, CM
VSAT		SC, CA, AC, CM
Remote Uplink Site		AT, AC, IA, PM, RA
Terrestrial Repeaters		SC, CA, CM, PE
Studio		AT, AC, CA, IA, RA, PE, PM
Mobile Receivers		SI
Sirius Satellite Constellation	Affected systems	CA, IA, AC, SI
VSAT		CA, IA, AC, SI
Remote Uplink Site		CA, AC, PM, SR
Terrestrial Repeaters		CA, AC, PM, SR
Studio		AC, AT, PE, PM, PS
Mobile Receivers		
Sirius Satellite Constellation	Discoverability	AU, MP, MA
VSAT		AU, MP, MA
Remote Uplink Site		AU, MP, MA
Terrestrial Repeaters		AU, MP, MA
Studio		MP, PE, AT
Mobile Receivers		MP

Table 7.4: Radio and TV Satellite Mitigation Controls

Component	**DREAD**	**Controls**
Starlink Satellite Constellation	Damage	CA, IA, AC, SI
Starlink Uplink Station		AC, IA, AT, IA, PS, SI, SC, PM
Starlink Dish Antenna		PE, SC
Router		SC, SI, SR
User Terminals		SC, CM, SR, SI
Starlink Satellite Constellation	Reproducibility	MA, AC, CM
Starlink Uplink Station		IR, MA, AC, AT, PE, PS, SC, PM
Starlink Dish Antenna		MA, CM
Router		MA, CA, CM, SR
User Terminals		SC, MA, CM
Starlink Satellite Constellation	Exploitability	SC, CA, AC, CM
Starlink Uplink Station		AT, AC, IA, PM, RA
Starlink Dish Antenna		PM, CM
Router		SC, SI
User Terminals		SC
Starlink Satellite Constellation	Affected systems	CA, IA, AC, SI
Starlink Uplink Station		CA, AC, PM, SR
Starlink Dish Antenna		AC, IA, PM
Router		SR
User Terminals		SI
Starlink Satellite Constellation	Discoverability	AU, MP, MA
Starlink Uplink Station		AU, MP, MA
Starlink Dish Antenna		MP
Router		MP
User Terminals		MP

Table 7.5: Starlink Mitigation Controls

Component	DREAD	Controls
Relay Satellite Ground Station User Observation Center	Damage	CA, IA, AC, SI AC, IA, AT, IA, PS, SI, SC, PM AC, IA, AT, IA, PS, SI, SC, PM
Relay Satellite Ground Station User Observation Center	Reproducibility	MA, AC, CM IR, MA, AC, AT, PE, PS, SC, PM IR, MA, AC, AT, PE, PS, SC, PM
Relay Satellite Ground Station User Observation Center	Exploitability	SC, CA, AC, CM AT, AC, IA, PM, RA AT, AC, IA, PM, RA
Relay Satellite Ground Station User Observation Center	Affected systems	CA, IA, AC, SI CA, AC, PM, SR CA, AC, PM, SR
Relay Satellite Ground Station User Observation Center	Discoverability	AU, MP, MA AU, MP, MA AU, MP, MA

Table 7.6: Earth Observation Mitigation Controls

7.3 Discussion

Due to the functional similarities among certain CPS elements, they have been assigned the same mitigation controls, even though they belong to different services. For example, all the satellite elements (GPS, Communication, Sirius, Starlink, and Relay) have identical Damage-reduction controls, because they all serve the same purpose in their respective CPS.

Because satellites are remote and inaccessible, the controls given to them are based on securing the communication they receive and send out. This includes things like Access Control and Identification and Authentication, to ensure the integrity of incoming signals and commands, and prevent spoofing and hijacking attacks. Maintenance through software updates is also an important countermeasure to avoid adversaries taking advantage of old software bugs and preventing satellites from becoming old vulnerable legacy systems. Media Protection is also an important aspect to consider, because of the security through obscurity principle that is often practiced in space systems. Any disclosure of this obscurity to the media and public could compromise system security.

Regarding elements in the ground segment, many of the same countermeasures apply, however, these elements are subject to additional threats due to their physical availability. Including mitigation controls like Physical and Environmental Protection, Personnel Security, Access Control, Awareness and Training, and Incident Response is therefore crucial to ensure physical security and avoid insider threats from employees.

In the case of the user segment and the UTs, management and monitoring of devices can be difficult for a satellite system owner or stakeholder, because the UTs often reside outside their system and control. Given that UTs in most cases are private mobile devices, the designated mitigation controls primarily address securing communication to and from these devices. This includes controls like System and Communications Protection, but also Supply Chain Risk Management, because UTs are a part of the supply chain.

While employing NIST's framework controls, some domain-specific mitigation measures might not be addressed. However, this compromise is necessary to adhere to an established framework compared to a less recognized one. By implementing these standardized controls, satellite systems' overall cybersecurity experiences significant enhancement, effectively mitigating the majority of existing threats.

Chapter 8 Conclusion

8.1 Results

The research conducted in this thesis revealed several key findings. Firstly, the current state of cybersecurity in orbital satellites is inadequate to meet the growing threat landscape. Many satellites lack basic security measures such as authentication and encryption, making them vulnerable to unauthorized access and data interception.

Further several interconnections between satellite systems and critical terrestrial infrastructure have been identified. There is no doubt that several critical infrastructures would fail to operate if their connected satellite system was disrupted. This raises the question about whether space systems and satellites should be considered as critical infrastructure or not, with several researchers promoting the decision to do so.

After deciding on an appropriate attack path methodology, several attack paths were identified in five different satellite services. However, in the individual systems few distinct paths from the entry node to satellite constellation existed. With this lack of redundance, the importance of securing these single paths and links cannot be underestimated.

Luckily, available countermeasures exist and was identified through NIST controls. If implemented, these controls would severely improve the current state of cybersecurity in satellite systems, which are crucial to secure to ensure the operation of several critical infrastructures.

8.2 Future Work

The field of cybersecurity in satellites and space systems are quite underdeveloped despite its importance. Potential further studies are therefore endless, however notable mentions related to the results and limitations of this thesis are:

- As this thesis is a relatively general overview of interconnections between satellites and terrestrial critical infrastructure, further investigation of satellites role and implementation in specific infrastructure systems would be interesting. This in order to better determine the criticality of satellites presence.

- Also, further development of space security frameworks and mitigation techniques would help securing space systems against an increasingly hostile threat landscape.

- Because this thesis mostly focuses on the possible paths from node to node in a satellite CPS, and discovered that inadequate redundancy exists, it would be interesting and beneficial to investigate the security of the links between these nodes.

- Another aspect that has not been considered in this thesis is the pre-launch operation. Because satellites are so remote once they reach space, an important security aspect is to ensure the correct configuration and calibration of the satellites before they are launched into space. If hardware and software flaws exist when the satellite gets launched, it will be hard to fix, and can therefore pose a huge security threat. Further research taking this into consideration would be beneficial.

References

[1] J. J. Plotnek, "A threat-driven resilience assessment framework and security ontology for space systems", Dec. 2022.

[2] J. J. Plotnek and J. Slay, "Space systems security: A definition and knowledge domain for the contemporary context", 2022.

[3] J. J. Plotnek and J. Slay, "A new dawn for space security", 2022.

[4] J. S. Fredheim, "Attack paths in critical space infrastructure", Nov. 2023.

[5] J. Pavur and I. Martinovic, "Sok: Building a launchpad for impactful satellite cyber-security research", Oct. 2020.

[6] G. Falco, "The vacuum of space cyber security", Sep. 2018.

[7] T. Harrison, K. Johnson, *et al.*, "Space threat assessment 2022", Apr. 2022.

[8] D. P. Fidler, "Cybersecurity and the new era of space activitiescybersecurity and the new era of space activities", 2018.

[9] SmartSat, "Smartsat 2022, satellite cyber resilience whitepaper, smartsat, adelaide, australia", Apr. 2022.

[10] V.-C. Matei, "Cybersecurity analysis for the internet-connected satellites", Dec. 2021.

[11] S. Shahzad, L. Qiao, and K. Joiner, "Need for a cyber resilience framework for critical space infrastructure", 2022.

[12] United Nations Sustainable Development Goals. [Online]. Available: https://sdgs.un.org/goals (last visited: Jun. 1, 2024).

[13] Systematic Literature Review or Literature Review? [Online]. Available: https://scientific-publishing.webshop.elsevier.com/research-process/systematic-literature-review-or-literature-review/ (last visited: May 27, 2024).

[14] Google Search Statistics. [Online]. Available: https://trends.google.com/trends/explore?date=all&q=cybersecurity%20in%20space,cybersecurity&hl=no (last visited: Feb. 20, 2024).

[15] J. G. Oakley, "Cybersecurity for space: Protecting the final frontier", 2020.

[16] S. S. Visner and P. Sharfman, "Development of cybersecurity norms for space systems", Nov. 2021.

[17] M. Manulis, C. Bridges, and R. Harrison, "Cyber security in new space", May 2020.

[18] Space hackers: myth vs. reality. [Online]. Available: https://www.kaspersky.com/blog/cybersecurity-in-outer-space/43531/ (last visited: Mar. 15, 2024).

[19] K.-U. Schrogl, "Handbook of space security", Oct. 2020.

[20] UCS Satellite Database. [Online]. Available: https://www.ucsusa.org/resources/satellite-database (last visited: Mar. 8, 2024).

[21] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. [Online]. Available: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/ (last visited: Feb. 21, 2024).

[22] M. Calabrese, "Space oddity: Space cybersecurity lessons from a simulated ops sat attack", Jul. 2023.

[23] W. Knowles, D. Prince, *et al.*, "A survey of cyber security management in industrial control systems", Jun. 2015.

[24] C. Kapalidis, C. M. Maple, *et al.*, "Cyber risk management in satellite systems", 2019.

[25] I. 23312:2022, "Space systems — detailed space debris mitigation requirements for spacecraft", Jul. 2022.

[26] Legacy Systems: Keeping Older Satellite Systems Operating. [Online]. Available: https://www.satellitetoday.com/connectivity/2008/01/01/legacy-systems-keeping-older-satellite-systems-operating/ (last visited: Mar. 15, 2024).

[27] A. Schalk, L. Bronik, and D. Brown, "Analysis of vulnerabilities in satellite software bus network architecture", 2022.

[28] T. C. C. for Space Data Systems, "Recommendation for space data system standards: Space packet protocol", Jun. 2020.

[29] Critical Infrastructure Sectors. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited: Feb. 22, 2024).

[30] Critical Infrastructure Council Directive. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114 (last visited: Feb. 22, 2024).

[31] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555#C1-1 (last visited: Jun. 3, 2024).

[32] U. G. P. Office, "Code of federal regulation, title 47, volume 3", Oct. 2005.

[33] CISA - Chemical Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/chemical-sector (last visited: Mar. 6, 2024).

[34] Critical Infrastructure: Space Security and Cybersecurity Intersect. [Online]. Available: https://www.captechu.edu/blog/part-1-critical-infrastructure-space-security-and-cybersecurity-intersect (last visited: Mar. 6, 2024).

[35] CISA - Commercial Facilities Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/commercial-facilities-sector (last visited: Mar. 7, 2024).

[36] Uses of Broadcast Communications Satellites. [Online]. Available: https://sia.org/satellites-services/broadcast-satellite-tv-radio/ (last visited: Mar. 7, 2024).

[37] CISA - Communications Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector (last visited: Mar. 7, 2024).

[38] We Have an Anomaly: America Is Missing a Space-Systems Critical Infrastructure Sector. [Online]. Available: https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/3540970/we-have-an-anomaly-america-is-missing-a-space-systems-critical-infrastructure-s/ (last visited: Mar. 7, 2024).

[39] CISA, "Introduction to the communications sector risk management agency", Aug. 2021.

[40] CISA - Dams Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/dams-sector (last visited: Mar. 7, 2024).

[41] Space technology helps boost dam safety. [Online]. Available: https://space.blog.gov.uk/2021/08/11/space-technology-helps-boost-dam-safety/ (last visited: Mar. 7, 2024).

[42] É. Daxhelet, "The intersection between outer-space security and cybersecurity", Jul. 2023.

[43] F. Cilufo, M. Montgomery, *et al.*, "Time to designate space systems as critical infrastructure", Apr. 2023.

[44] Military Satellites by Country 2024. [Online]. Available: https://worldpopulationreview.com/country-rankings/military-satellite-by-country (last visited: Mar. 8, 2024).

[45] D. P. Andrews, R. V. Davis, *et al.*, "Commission to assess united states national security space management and organization", Jan. 2001.

[46] CISA - Defense Industrial Base Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector (last visited: Mar. 7, 2024).

[47] CISA, "Defense industrial base sector-specific plan: An annex to the national infrastructure protection plan", May 2010.

[48] CISA - Emergency Services Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector (last visited: Mar. 11, 2024).

[49] 6 Satellite Services That Critical Infrastructure Depends On. [Online]. Available: https://anchoramconsulting.com.au/blog/f/6-satellite-services-that-critical-infrastructure-depends-on (last visited: Mar. 11, 2024).

[50] M. E. Lucarelli, "Satellite services: Communications for disasters and emergency response", Mar. 2019.

[51] Satellite: The “Go To” Solution for Resilient Emergency Response Communications. [Online]. Available: http://www.satmagazine.com/story.php?number=1950983317 (last visited: Mar. 11, 2024).

[52] CISA - Food and Agriculture Sector. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector (last visited: Mar. 11, 2024).

[53] Benefits of Space: Agriculture. [Online]. Available: https://www.unoosa.org/oosa/en/benefits-of-space/agriculture.html (last visited: Mar. 11, 2024).

[54] A. Georgescu, U.-E. Botezatu, *et al.*, “Critical infrastructure dependency on space systems”, Jun. 2016.

[55] CISA, “Information technology sector-specific plan: An annex to the nipp 2013”, 2016.

[56] GNSS. [Online]. Available: https://snl.no/GNSS (last visited: Mar. 12, 2024).

[57] What is ITS? [Online]. Available: https://its-norway.no/en/about-its-norway/what-is-its/ (last visited: Mar. 12, 2024).

[58] F. Peyret, P.-Y. Gilleron, and L. Ruotsalainen, “Better use of global satellite systems for safer and greener transport”, Sep. 2015.

[59] E. Wallischeck, “Gps dependencies in transportation”, Aug. 2016.

[60] S. Katsikas and G. Kavallieratos, “Attack path analysis for cyber physical systems”, *Computer Security*, pp. 19–33, Oct. 2020.

[61] S. Katsikas, C. Lambrinoudakis, *et al.*, “Computer security. esorics 2021 international workshops: Cybericps, secpre, adiot, spose, cps4cip, and cdt&secomane, darmstadt, germany, october 4–8, 2021, revised selected papers”, vol. 13106, 2022.

[62] N. Polatidis, M. Pavlidis, and H. Mouratidis, “Cyber-attack path discovery in a dynamic supply chain maritime risk management system”, *Computer Standards & Interfaces*, vol. 56, pp. 74–82, 2018.

[63] C. Cheh, K. Keefe, *et al.*, “Developing models for physical attacks in cyber-physical systems”, pp. 49–55, 2017.

[64] H. Mouratidis and V. Diamantopoulou, “A security analysis method for industrial internet of things”, *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4093–4100, 2018.

[65] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, “Assessing iot enabled cyber-physical attack paths against critical systems”, *Computers & Security*, vol. 107, p. 102 316, 2021.

[66] K. Thangavel, J. J. Plotnek, *et al.*, “Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity”, Oct. 2022.

[67] A. Akbarzadeh and S. Katsikas, “Identifying critical components in large scale cyber physical systems”, Sep. 2020.

[68] G. Kavallieratos and S. Katsikas, “An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space”, Dec. 2023.

[69] GPS Space Segment. [Online]. Available: https://www.gps.gov/systems/gps/space/ (last visited: Apr. 11, 2024).

[70] GPS Control Segment. [Online]. Available: https://www.gps.gov/systems/gps/control/ (last visited: Apr. 11, 2024).

[71] GPS User Segment. [Online]. Available: https://www.gps.gov/applications/ (last visited: Apr. 11, 2024).

[72] Y. Su, Y. Liu, *et al.*, "Broadband leo satellite communications: Architectures and key technologies", Apr. 2019.

[73] Sirius XM. [Online]. Available: https://en.wikipedia.org/wiki/Sirius_XM (last visited: Apr. 11, 2024).

[74] S. DiPierro, R. Akturan, and R. Michalsk, "Sirius xm satellite radio system overview and services", Sep. 2010.

[75] World's Most Advanced Broadband Satellite Internet. [Online]. Available: https://www.starlink.com/technology (last visited: Apr. 11, 2024).

[76] Starlink Network Topology. [Online]. Available: https://medium.com/@jaykrs/starlink-network-topology-289dd3ddb14d (last visited: Apr. 11, 2024).

[77] SpaceX – Starlink System Architecture for Internet. [Online]. Available: https://www.techplayon.com/starlink-system-architecture/ (last visited: Apr. 11, 2024).

[78] Q. Zhao, L. Yu, *et al.*, "An overview of the applications of earth observation satellite data: Impacts and future trends", Apr. 2022.

[79] J. Letschnik, K. Raif Matthias an Pauly, and U. Walter, "Bayernsat – a real-time communication- architecture for interactive earth observation via geostationary inter satellite link for small satellite systems", Apr. 2005.

[80] G. Kavallieratos, G. Spathoulas, and S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems", Mar. 2021.

[81] K. Stouffer, M. Pease, *et al.*, "Nist sp 800-82r3 - guide to operational technology (ot) security", Sep. 2023.

[82] E. Gugliandolo, "Critical infrastructure protection in the space sector a 2030 outlook", Apr. 2024.

[83] Space Attack Research & Tactic Analysis (SPARTA). [Online]. Available: https://sparta.aerospace.org/ (last visited: May 27, 2024).

NTNU

Norwegian University of
Science and Technology