Master of Science in Engineering: Computer Security
May 2023

Secure satellite internet usage in high-risk areas

Carl Johansson
Andreas Kvant

Faculty of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Engineering: Computer Security. The thesis is equivalent to 20 weeks of full-time studies.

The authors declare that they are the sole authors of this thesis and that they have not used any sources other than those listed in the bibliography and identified as references. They further declare that they have not submitted this thesis at any other institution to obtain a degree.

Contact Information:
Author(s):
Carl Johansson
E-mail: calle94johansson@hotmail.com

Andreas Kvant
E-mail: kvant040@hotmail.com

University advisor:
Dr Lars Lundberg
Department of Computer Science

Faculty of Computing
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Abstract

Background. In high-risk areas, a reliable and secure internet connection is not always guaranteed. If the terrestrial internet infrastructure is damaged due to armed conflicts in the area, the internet is shut down or internet traffic is monitored by antagonistic parties, satellite internet technology could be a suitable alternative for people or organizations operating in these areas. However, satellite internet comes with its own advantages and shortcomings, and if satellite internet systems are going to be used in these areas, there is a need for secure utilization of the system and awareness of possible vulnerabilities, threats, and risks of using them.
Objectives. There are four main objectives of this study: (1) To identify the general threats and vulnerabilities that accompany the use of satellite internet technology in a high-risk area. (2) To assess the risks to the user's safety that may come as a consequence of the vulnerabilities being exploited or threats being realized. (3) To identify possible mitigations to the risks, and device best practices for the secure use of satellite internet technology in high-risk areas. (4) Produce a document that provides information about satellite internet technology, clarifies what vulnerabilities, threats, and risks could be present when using satellite internet in a high-risk area and how the user may assess the risk according to their own situation, the document should also provide the user with mitigations and best practices for the secure use of the satellite internet technology in order to ensure the user's safety.
Methods. A structured literature review, semi-structured interviews, and multiple threat analysis methods were used to gather and evaluate the threats to satellite internet. The literature review presented the previous research done, and the interviews gave some perspectives from the industry. The results were then compiled into a document which we evaluated in a workshop to determine its usability and get feedback we could use to improve it.
Results. The results show that satellite internet systems are exposed to several attacks, and tracking was a discovered threat that was not mentioned in previous research. When making our example risk assessment tracking also received the highest score, due to it allowing an adversary to threaten the physical safety of a user.
Conclusions. The interest in satellite internet security research seems to have recently increased. The most exposed part of the satellite internet infrastructure is the wireless communication link, especially in high-risk areas where attacks targeting the radio signal are more prevalent. User awareness was our most important mitigation against the threats found and is the core contribution of this work.

Keywords: satellite internet, high-risk area, threats, risks, mitigations.

Sammanfattning

Bakgrund. Att pålitlig och säker internetuppkoppling är tillgänglig i högriskområden är inte alltid garanterat. Om den markbaserade internetinfrastrukturen skadas på grund av väpnade konflikter i området, internet stängs ned eller internettrafiken övervakas av antagoniska parter, så är satellitinternetteknologi ett lämpligt alternativ för personer eller organisationer som verkar i dessa områden. Satellitinternet har dock sina egna fördelar och nackdelar. Om dessa system ska användas i högriskområden är det av yttersta vikt att de används säkert och att användaren är medveten om vilka möjliga sårbarheter, hot och risker som ackompanjerar användningen av systemen.
Syfte. Det finns fyra mål med detta arbete: (1) Att identifiera de allmänna hot och sårbarheter som ackompanjerar användningen av satellitinternetteknologi i ett högriskområde. (2) Att bedöma de risker mot användarens säkerhet som kan uppstå till följd av att sårbarheterna utnyttjas eller hoten realiseras. (3) Att identifiera möjliga åtgärder för att mitigera riskerna och utveckla bästa praxis för den säkra användningen av satellitinternetteknologi i högriskområden. (4) Att producera ett dokument som tillhandahåller information om satellitinternetteknologi, klargör vilka sårbarheter, hot och risker som kan förekomma vid användning av satellitinternet i högriskområden samt hur användaren kan bedöma risken utefter sin egen situation. Dokumentet bör också ge användaren åtgärder mot risker och bästa praxis för säker användning av satellitinternetteknologi samt att säkerställa användarens säkerhet.
Metoder. En strukturerad litteraturstudie, semi-strukturerade intervjuer och flera hotanalysmetoder användes för att samla in och utvärdera hoten mot satellitinternet. Litteraturstudien presenterade tidigare forskning och intervjuerna gav några perspektiv från branschen. Resultaten sammanställdes sedan i ett dokument som vi utvärderade i en workshop för att bestämma dess användbarhet och få feedback vi kunde använda för att förbättra det.
Resultat. Resultaten visar att satellitinternetsystem kan utsättas för flera attacker, och spårning var ett hot vi upptäckte som inte nämnts i tidigare forskning. I vår exempelriskbedömning fick spårning också den högsta poängen, eftersom det möjliggör för en motståndare att påverka en användares fysiska säkerhet.
Slutsatser. Resultaten visar att satellitinternetsystem kan utsättas för flera attacker, och spårning var ett hot vi upptäckte som inte nämnts i tidigare forskning. I vår exempelriskbedömning fick spårning också den högsta poängen, eftersom det möjliggör för en motståndare att påverka en användares fysiska säkerhet.

Nyckelord: satellit internet, högrisk områden, hot, risker, åtgärder.

Acknowledgments

We would like to thank *Knowit cybersecurity and Law*, their employees, and our company supervisors Victor Langåssve and Elin Wallgren, for their support, motivation, and expertise throughout our master's thesis project. We would also like to thank the employees at *Civil Rights Defenders*, and especially our main contact Niklas Lindhé for providing feedback and rewarding discussions for this project's final result. Last but not least we want to thank our academic supervisor at *Blekinge Technical Institute of Technology*, Lars Lundberg for his support, guidance, and supervision, keeping us on the right track throughout this project.

Contents

List of Figures

List of Tables

Abbreviations

BTH Blekinge Institute of Technology. 20

CIA Confidentiality, Integrity and Availability. 3, 4, 25, 37

CRD Civil Rights Defenders. 1, 4, 20, 26, 40, 47, 50

CVSS Common Vulnerability Scoring System. 24

DoS Denial-of-Service. 14, 32, 33, 43, 46, 54

DTN Delay- and Disruption-Tolerant Networking. 15

GEO Geostationary Earth Orbit. 5, 6, 13

HTS High-Throughput Satellite. 11

IP Internet Protocol. 15, 28

ISP Internet Service Provider. 5, 44, 56

LEO Low Earth Orbit. 5–8, 14

MEO Medium Earth Orbit. 5

NGEO Non-Geostationary Earth Orbit. 5

PASTA Process for Attack Simulation and Threat Analysis. 24

SLR Structured Literature Review. xiii, 3, 11, 17, 18, 23, 24, 27–31, 40, 43, 44, 49

STRIDE Spoofing, Tampering, Repudiation, Information-Disclosure, Denial-of-service and Elevation-of-privilege. 24, 31

Chapter 1

Introduction

In the interconnected world of today, access to the internet, as well as reliable communication, has become an essential and obvious necessity for individuals, organizations, and governments. However, in high-risk areas like warzones, disaster-stricken areas, dictatorships, or terrorist-occupied land, traditional forms of communication and internet access are not guaranteed. In these zones, the terrestrial internet network may be unavailable due to infrastructure damage, government control, or unreliable due to the networks being monitored or shut down [46] [45]. People who operate in these zones, like activists and journalists for example, who work for the promotion of human rights, democracy, and freedom of the press have high reliability on communication channels and internet connectivity. They require reliable and trustworthy communication channels to coordinate their efforts and communicate with the outside world, to share information, or get help from the international community [44].

The organization Civil Rights Defenders (CRD) [9], which has many clients who work in high-risk areas, sees the emergence of satellite-based internet as a potential solution to many of the issues related to the terrestrial internet. With satellite internet, people who work in these high-risk areas would not need to rely on the terrestrial internet infrastructure to communicate. This project is grounded in CRD having an interest in how the technology of satellite internet could benefit their clients in high-risk areas, and if satellite internet is something they should provide for their clients.

With this in mind, there are many important aspects one needs to consider, including availability, reliability, and security as well as providing confidentiality and integrity in the systems they would want to use for this purpose. These aspects are especially important in high-risk areas like a warzone or dictatorship where there are potential adversaries that may seek to shut down, jam, eavesdrop, or otherwise alter the satellite communication to sabotage the opposing party [26]. Besides the potential loss or otherwise compromise of data, it is also important that people are not put in any physical danger due to using satellite internet when operating in these zones.

Therefore this project aims to provide a practical guide that assesses the vulnerabilities, threats, and risks that may be involved when considering using satellite internet to communicate in a high-risk area. The guide is meant to provide general information about satellite internet systems, present the threats and vulnerabilities associated with the use of the satellite internet system in a high-risk area as well as an example risk assessment which contains reasoning of the risks so that the user may understand them better. Additionally, this document is meant to provide guide-

lines for best practices as well as methods and tools to establish and maintain secure communication for the user of the satellite system.

1.1 Aim, objectives, and research questions

This work aims to provide a practical document that may act as a risk assessment guide for the usage of satellite internet in a high-risk area. This document, which we have chosen to call a practical guide, consists of two parts: The first part of the practical guide is an analysis of the security seen from the user side of satellite systems. This part looks at the different parts of the satellite internet infrastructure including the user terminal and equipment, the satellite itself, the ground-station gateway, and also the communication links tying the different parts together. The purpose of this part is to determine what vulnerabilities and threats exist in the different components of the system, and what the potential risks are that may come as a result of these vulnerabilities and threats. The second part of the practical guide details the potential mitigations to these risks as well as user guidelines such as potential best practices, methods, and tools for using satellite internet in as secure a way as possible for the user. The intention is for this practical guide to be used by individuals or organizations who operate or intend to conduct operations in a high-risk area. The document is intended to assist them in making an informed initial decision on whether satellite internet is a viable communication option for them or not, as well as provide them with helpful information and guidelines regarding the risks of utilizing satellite internet in a high-risk area should they intend to do so. Several objectives need to be investigated to be able to create this guide. These objectives are:

- To identify what the requirements are regarding satellite internet security for a person who operates in a high-risk area.
- To map out general vulnerabilities and threats that may be present when using satellite internet in a high-risk area.
- To find out the risks related to the vulnerabilities and threats found in association with using satellite internet in a high-risk area. For example, if the satellite signal is visible to militaries participating in a war, and if it can turn a civilian into a potential target of an attack.
- To find ways to mitigate the identified risks, and deduce best practices that may assist in preventing insecure situations.

This leads to the research questions created from the objectives to reach the aim of this work:

RQ1 *What vulnerabilities and threats exist that are related to any part of the satellite internet infrastructure that can have a negative impact on a user of satellite internet technology in a high-risk area?*

RQ2 *What are the risks of using satellite internet communication in a high-risk area that may come as a consequence of the vulnerabilities and threats found in satellite internet infrastructure?*

RQ3 *What measures can be taken by a user to mitigate the risks of using satellite internet in a high-risk area found in RQ2?*

1.2 Scope and Limitations

The practical guide which is created as a result of this work targets users of satellite internet in high-risk areas. A focus was therefore on threats that target users, and can be mitigated by the user themselves. Considering the possibility of terrestrial internet infrastructure being damaged or otherwise unavailable to a user located in high-risk area, this work is focused on satellite internet technology wherein there is both an uplink and downlink established between the satellite and user terminal.

While satellite internet can be considered an extension of terrestrial internet, any threats originating from regular use of internet is not within the scope of this work, instead the scope is only focused on this extension.

1.3 Structure

The structure of the rest of this thesis is outlined below:

- **Background** - In this chapter, we present an introduction to the problem as well as a description of the research gap related to satellite communication in high-risk areas. Furthermore, there is an overview of satellite internet communication systems, the different parts of the systems and their connections as well as the general differences between terrestrial internet infrastructure, satellite internet infrastructure, and how they tie into one another.

- **Related Work** - In this chapter, we present the work related to the scope of our thesis that has been found in the Structured Literature Review (SLR), as well as a summary of each related work.

- **Method** - In this chapter, we describe the methodologies used in the SLR as well as the structuring of the interviews and formulation of the interview questions. We will also describe the method used for threat categorization, risk assessment, and the use of the Confidentiality, Integrity and Availability (CIA) triad to further categorize the risks. We also explain how the practical guide is put together and the way it is evaluated for usability.

- **Results** - In this chapter, we present the results discovered in the SLR and the interviews relating to each of our research questions. We also present the results of the risk assessment done in this project, and finally, we present the resulting Practical Guide and the result of its evaluation.

- **Analysis and Discussion** - In this chapter, we analyze the results found in the SLR and interviews. We also discuss threat categorization, risk assessment,

and our use of the CIA triad. We also discuss the practical guide, and its usability from the perspectives of the employees of CRD, as well as discuss what feedback that was implemented or not, and why, in the revised version of the practical guide. In this chapter, we will also discuss potential validity threats against this study.

- **Conclusion and Future Work** - In this chapter, we present the conclusion to our research in relation to the research questions and also present some possible future work related to the topic of this study.

Chapter 2

Background

This chapter presents some background information on satellite-based internet networks, information on how these systems operate as well as a comparison between satellite internet infrastructure and terrestrial internet infrastructure. Additionally, we also present the problems and shortcomings prevalent in satellite systems and how they relate to our thesis topic.

2.1 Satellite based internet

Satellite-based internet is a broadband internet service that uses satellites in orbit to relay signals between a user's dish antenna and the Internet Service Provider (ISP) ground station. This technology is especially useful in remote or high-risk areas where the traditional terrestrial internet infrastructure, such as cables or cell towers, may be unavailable or unreliable [46].

There are two main types of satellites used for internet connectivity, these are Geostationary Earth Orbit (GEO) satellites and Non-Geostationary Earth Orbit (NGEO). The NGEO satellites are then further divided into Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellites. GEO satellites are positioned at a fixed position, in a location above the Earth's equator about 36000 km above Earth. This gives them coverage of about a third of the Earth's surface when sending and receiving signals, while NGEO satellites orbit Earth at a much lower altitude. MEO satellites sustain their orbit at an altitude of about 2000 km above the surface, up to the height of GEO satellites, and LEO satellites sustain their orbit on an altitude of around 200-2000 km [15].

The infrastructure of satellite-based internet consists of three main components: the user equipment, the satellite, and the ground segment. The user equipment includes a dish antenna, a modem, and a router which is installed at the user's location. The ground segment includes the ISP's ground station and their gateway to the internet backbone [16]. The satellite itself relays signals with radio waves between the user equipment and the ground segment. Several different radio wave signals are used by satellites with the most common ones being: C-band (4-8 GHz) Ku-band (10-18 GHz), and Ka-band (18-31 GHz). The higher the frequency the smaller the dish antenna is needed to receive the signal [15]

The process of transmitting data over satellite-based internet begins with the user's request for a web page or other online resource. The user's dish antenna receives the request and transmits it to the satellite, which relays it to the ISP's ground station. The ground station processes the request and retrieves the requested

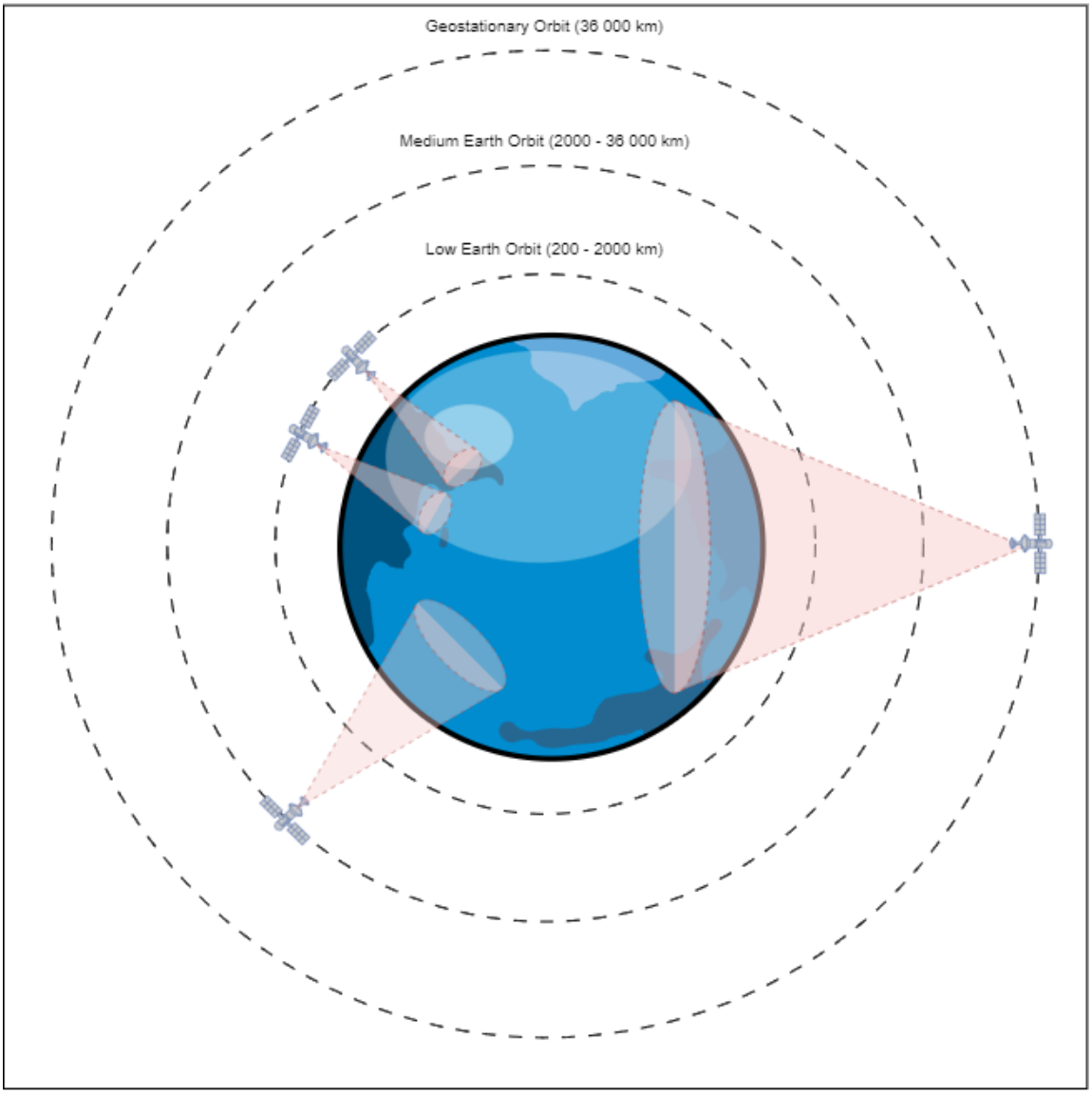

Figure 2.1: An illustration of GEO, MEO, and LEO satellites, their orbit, and their coverage

data from the internet backbone. The requested data is then transmitted to the satellite, which relays it to the user's dish antenna. The modem and router in the user's equipment then decode the data and distribute it to the user's devices [15].

As long as the user has a clear line of sight to the satellite, they can access the internet from virtually anywhere on the planet. This makes it a valuable tool for disaster response and recovery, as well as for providing internet access to remote or underserved communities. However, satellite-based internet also has some limitations, such as higher latency (delay) and lower bandwidth (data transfer rate) compared to terrestrial connections, due to the long distance that signals have to travel between Earth and the satellite [16].

LEO satellites have some advantages over GEO satellites, such as lower latency and higher bandwidth, compared to their proximity to Earth. However, LEO satellite systems require a larger number of satellites to provide continuous coverage, and the

satellites need to move at high speeds to remain in orbit, which can make it more difficult to track them and maintain a stable connection. Nonetheless, LEO satellite internet providers are emerging as a competitive alternative to traditional internet services in some areas, especially where the geography makes it difficult to lay cables or erect cell towers [16].

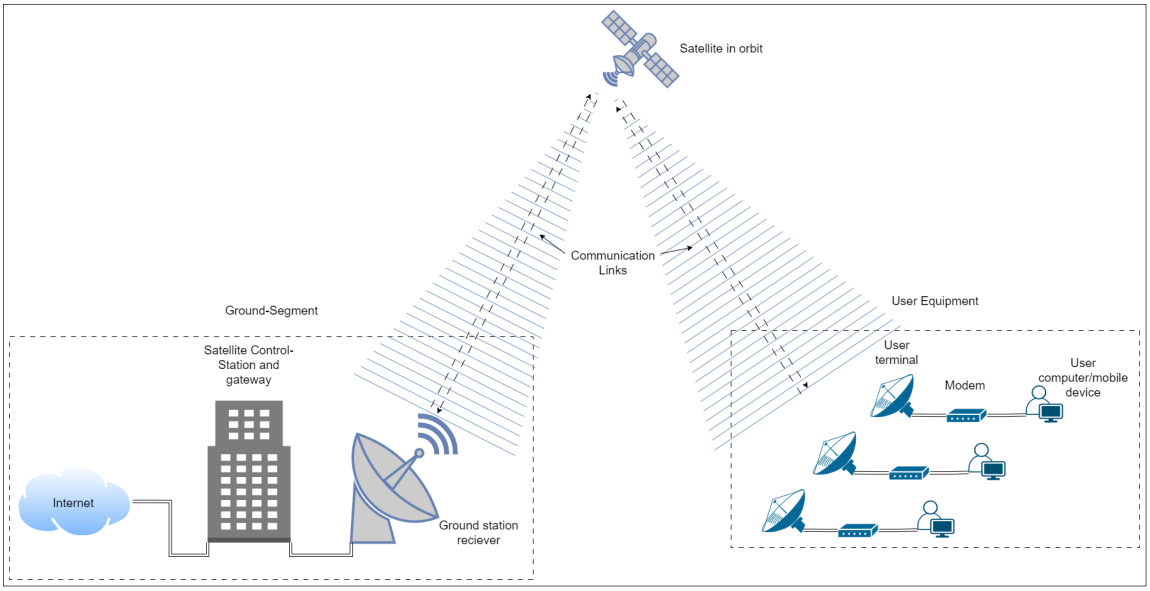

Figure 2.2: Satellite internet infrastructure

2.2 Terrestrial internet vs satellite internet and the new satellite constellations

Terrestrial internet typically offers faster speeds and higher bandwidth with no data caps because data only needs to travel through physical infrastructure that is typically closer to the user, however, the coverage is limited to areas where infrastructure has been installed. [16]

Satellite internet on the other hand provides wider coverage and can be accessed from virtually anywhere with a clear view of the sky, making it a suitable option for remote and rural areas where terrestrial internet is not available. Though the drawback is that satellite internet often has higher latency due to the long distance data must travel to reach the satellite and back, which can cause delays in applications requiring low latency such as online gaming or video conferencing limiting its usefulness for heavy internet users [16].

That being said, in comparison to traditional satellite internet, the new satellite constellation networks in LEO, such as Starlink[1], offer several advantages in terms of speed, latency, and bandwidth. Unlike traditional satellite internet, Starlink and other LEO satellite constellations have satellites that orbit much closer to Earth, resulting in significantly lower latency. This makes LEO satellite internet much more

[1]https://www.starlink.com/technology

responsive, with speeds and latency comparable to or even better than terrestrial internet. In terms of bandwidth, the LEO satellite constellations have more bandwidth capacity than traditional satellite internet, making it a more viable option for heavy internet users. Additionally, because the satellites in the constellation are closer to Earth, the coverage area is smaller, which means that the total number of users sharing the same bandwidth capacity is reduced, resulting in faster and more reliable speeds [27].

However, there are still some limitations with LEO satellite internet, particularly in terms of coverage. While the coverage area is still wider than traditional terrestrial internet, it is not as extensive as traditional satellite internet, making it more challenging to access in very remote areas. Additionally, because the constellation is still being built, the network is not yet fully operational and may experience some disruptions or outages. This is an issue that needs to be addressed as the network continues to develop [4].

Satellite internet is also being more and more integrated to support the terrestrial network. Al Homssi et al. [4] discuss the integration of next-generation satellite internet with terrestrial internet infrastructure as an important aspect of providing ubiquitous and seamless connectivity. They note that the integration can be achieved through the use of gateways that connect the satellite network to terrestrial networks, such as fiber-optic cables, cellular networks, and Wi-Fi hotspots.

The authors point out that the integration of satellite and terrestrial networks can enhance the performance and reliability of the overall network, as it allows traffic to be routed dynamically between different access points based on network conditions and user requirements. In addition, the integration can help reduce latency and improve the quality of service by minimizing the number of satellite hops needed to transmit data.

The authors also mention the challenges associated with integrating satellite and terrestrial networks, such as the need for interconnection standards, bandwidth allocation, and management of network congestion. They suggest that the integration of satellite and terrestrial networks requires collaboration between different stakeholders, including satellite operators, terrestrial network providers, and regulatory authorities.

2.3 Satellite internet in high-risk zones

As mentioned, satellite internet is a technology that could provide internet connectivity to remote and hard-to-reach areas, it is increasingly being used to provide connectivity in high-risk areas where traditional infrastructure is disrupted or nonexistent. This has led to concerns regarding privacy, security, and cyber attacks on the communication network.

One example of the use of satellite internet in a war zone is Ukraine, where the ongoing conflict disrupted traditional internet infrastructure, prompting the Ukrainian government to turn to satellite internet as a solution. It was reported that satellite internet has provided a lifeline for many people in war-torn regions of Ukraine, demonstrating its potential as a tool for providing connectivity in difficult environments [21].

However, satellite internet has also posed challenges for the Ukrainian government and aid organizations due to its high cost and limited bandwidth, making it difficult to provide access to everyone who needs it [21]. Moreover, the use of satellite internet raises privacy and security concerns, as it is easier for governments and other actors to monitor and intercept satellite communication [5].

The potential for cyber attacks on satellite internet infrastructure has also been a concern. A report revealed that hackers targeted government and military entities by attacking satellite communication terminals in Europe [34].

Additionally, the use of satellite internet has led to political tensions. For instance, Iran reportedly blocked internet access for some users in August 2021 following the nationwide protests over the tragic killing of Mahsa Amini. This led the United States to issue a joint statement condemning the internet shutdowns in Iran and calling for the free flow of information [46]. In the wake of the internet shutdown in Iran, a campaign to smuggle satellite internet terminals into the country was initiated to provide the nation with internet access to the outside world [44].

So, while satellite internet shows promise in providing connectivity to high-risk areas such as war zones and disaster-stricken regions, it also poses challenges such as high costs, limited bandwidth, security concerns, and a high potential for cyber attacks. Governments, aid organizations, and other entities using satellite internet need to be aware of these issues and take appropriate measures to mitigate them.

Chapter 3

Related Work

This chapter presents the previous work related to this study that takes a similar approach or deals with similar issues. The works presented in this chapter have been extracted from a Structured Literature Review described in Section 4.1. They have been sectioned into previous reviews, surveys and data analysis studies, practical and experimental studies, and finally studies that propose some form of solution to a problem regarding the security of satellite internet. The purpose of this chapter is to also present the sources of the vulnerabilities, threats, risks, and risk mitigations that were used for risk assessment and threat analysis in this study and that also correlates to the research questions introduced in Section 1.1.

3.1 Previous reviews, surveys, and data analysis

Ma et al. [24] analyzed the security threats to the High-Throughput Satellite (HTS) communication system, including jamming, interception, and eavesdropping, as well as proposed countermeasures to mitigate these threats. They recommended using frequency hopping and directional antennas to address jamming attacks and encryption and authentication to secure the communication between the satellite and ground station. The authors conducted a literature review of existing research on the security of HTS communication systems and identify potential security threats. They then analyzed data on the performance of HTS communication systems under different threat scenarios and used simulation techniques to evaluate the effectiveness of various countermeasures.

Jang et al. [17] conducted a survey of physical layer security schemes in satellite networks to address security threats such as jamming, eavesdropping, and interference. They found that beamforming can improve the signal-to-noise ratio and reduce interference, artificial noise can confuse eavesdroppers, and cooperative jamming can improve the security of the system.

Ahmad et al. [3] discuss the unique vulnerabilities of satellite communications compared to terrestrial communications, such as longer propagation delays, wide coverage areas, and limited physical access control. The authors discuss the recurring challenge of applying the same technologies used in the ground network, such as TCP (Transfer Control Protocol) or TLS/SSL (Transport Layer Security/Secure Sockets Layer), in satellite communication since they are more error-prone due to the higher latency. The authors also identify various security threats to satellite communications, including interference, jamming, eavesdropping, and physical attacks. To mitigate these threats, the authors suggest various solutions such as encryp-

tion, frequency hopping, and diversity techniques, but they conclude that the use of encryption technologies in all types of communication involving satellites becomes difficult to deploy due to the latency.

Lohani and Joshi [23] investigated the security challenges facing satellite networks. The authors highlighted the vulnerabilities and threats posed by physical attacks and cyber-attacks on satellite systems. Physical threats were not relevant to this study, but the authors establish that data interception including hacking, jamming, spoofing, and denial of service attacks, is the most effective type of cyber-attack against satellite communication. The authors also discussed the need for security measures to protect satellite systems from these threats, including encryption, authentication, and access control mechanisms, they also suggest that these issues can be resolved by the use of quantum cryptography and mention that China has successfully tested this.

Wu et al. [50] conducted a review of threat analysis for space information networks based on network security attributes. They identified various types of threats, including information leakage, denial of service attacks, and unauthorized access, and discussed their impacts on the network. They also proposed several approaches to mitigate these threats, such as intrusion detection, access control, and data encryption.

Thangavel et al. [42] investigated adversary threats and countermeasures in the context of space cybersecurity. They discussed various types of threats, including denial of service attacks, malware, and unauthorized access, and proposed countermeasures such as authentication, access control, and encryption. They also presented a framework for analyzing the security of space systems.

Guo et al. [13] conducted a survey on space-air-ground-sea integrated network security in 6G. They discussed the unique security challenges of such integrated networks, such as interference, attacks on the routing protocol, and attacks on the wireless channel. They also proposed several solutions to mitigate these threats, such as secure routing protocols, intrusion detection systems, and physical layer security mechanisms.

Zhuo et al. [52] conducted a survey on security issues of routing and anomaly detection for space information networks. They discussed the vulnerabilities and threats to routing protocols and anomaly detection systems, as well as proposed several solutions to mitigate these issues. They also identified several challenges in securing space information networks, including limited resources, communication delays, and dynamic topology.

Manulis et al. [26] discussed cybersecurity in the context of new space, which refers to the emerging private sector space industry. They highlighted the importance of cybersecurity in ensuring the safety and sustainability of new space operations and discussed various security challenges, such as the need to secure satellite communication links, protect ground stations, and ensure the confidentiality and integrity of data. They also proposed several solutions to address these challenges, including secure communication protocols, encryption, and access control.

Schilling and Dmitrienko [40] proposed a comprehensive approach to increase security in satellite networks. They discussed various security vulnerabilities and threats, such as jamming attacks, data injection attacks, and physical attacks, and proposed several solutions to mitigate these issues. They also presented a framework

for assessing the security of satellite networks, which includes threat modeling, risk assessment, and security testing. The study involves a combination of simulation-based experiments and theoretical analysis to investigate and evaluate the performance of a proposed security mechanism for satellite networks.

Bradbury et al. [7] identified attack surfaces in the evolving space industry using reference architectures. They discussed the various components of space systems, such as ground stations, satellites, and communication links, as well as identified the potential vulnerabilities and attack surfaces associated with each component. They also proposed several solutions to mitigate these vulnerabilities, such as using secure communication protocols, implementing access control, and conducting security testing.

Scanlan et al. [39] discussed the potential increase in cyber risk that may arise from the deployment of new internet satellite constellations in industries that are ill-prepared for the associated cybersecurity challenges. They identified the risks associated with such constellations, such as network congestion, data loss, and data breaches, and highlighted the importance of developing appropriate cybersecurity measures to mitigate these risks.

He et al. [14] conducted a security analysis of a space-based wireless network. They identified the potential threats to the network, such as jamming attacks and eavesdropping, and proposed several solutions to mitigate these threats, such as using encryption and authentication protocols, implementing intrusion detection systems, and developing secure routing protocols. They also highlighted the importance of ongoing security testing and evaluation to ensure the network remains secure.

3.2 Previous studies involving practical or experimental approaches

In this section, the studies where a more practical or experimental approach has been taken are presented. To determine whether there has been a significant change in satellite communications security in recent years.

Pedersen et al. [33] conducted a security analysis of satellite communication systems operating in a GEO. The authors presented a threat model and analyzed potential attacks that could compromise the confidentiality, integrity, and availability of communication links between satellites and ground stations. The study focused on several aspects, including encryption protocols, key management, authentication mechanisms, and physical security. The authors also proposed countermeasures to mitigate the identified risks and improve the overall security of satellite communication systems in GEO.

Baselt et al. [6] investigated the security and privacy challenges of satellite communication in the aviation domain. The authors presented a threat model for satellite-based communication systems in aviation and analyzed potential vulnerabilities that could compromise the confidentiality, integrity, and availability of such systems. The study focused on several aspects, including air traffic control, cockpit communication, and passenger connectivity. The authors proposed countermeasures to mitigate the identified risks, such as the use of encryption, digital signatures, and

intrusion detection systems.

Santangelo et al. [38] proposed a cybersecurity "sandbox" platform to test small satellite vulnerabilities within the community. The authors presented the design and implementation of the LinkStar Cybersecurity Sandbox, a cloud-based environment that allows researchers and practitioners to simulate attacks on small satellite communication systems and evaluate the effectiveness of security measures. The study also presented updates and lessons learned from the deployment and use of the sandbox platform. The authors discussed several scenarios tested in the platform, such as Denial-of-Service (DoS) attacks, data exfiltration, and command injection.

Giuliari et al. [12] presented a study on attacking LEO satellite networks. The authors proposed the ICARUS framework, which uses a combination of passive and active techniques to identify and exploit vulnerabilities in LEO satellite networks. The study focused on several aspects, including the analysis of satellite communication protocols, the identification of attack surfaces, and the design of attack scenarios. The authors evaluated the effectiveness of the ICARUS framework through simulations and experiments on real-world satellite systems. The research highlights the need for improved security measures in LEO satellite networks.

Pavur et al. [32] presented a study on privacy and infrastructure security in Digital Video Broadcasting-Satellite (DVB-S) broadband. The authors analyzed the security and privacy risks associated with DVB-S technology, which is commonly used to provide internet access in remote areas. The study focused on several aspects, including the design of the DVB-S protocol, the identification of vulnerabilities in satellite ground stations, and the analysis of user data privacy. The authors proposed countermeasures to mitigate the identified risks, such as the use of encryption and secure communication channels. The findings can help improve the security and privacy of DVB-S satellite broadband and have implications for satellite communication systems in general.

Adelsbach and Greveler [2] conducted a study on the privacy risks associated with satellite communication systems. The authors analyzed several attack scenarios that could compromise the confidentiality and integrity of satellite communication channels, such as eavesdropping, replay attacks, and message modification. The study focused on the vulnerabilities of LEO satellite systems, which are commonly used for remote sensing and scientific research. The authors proposed several countermeasures to enhance the security of satellite communication, such as the use of encryption, authentication, and secure key exchange protocols. This study highlights the need for improved security measures in satellite communication systems to prevent unauthorized access and protect user privacy.

3.3 Proposed solutions

In this section, the studies that propose any form of a new solution, framework, or mitigation to solve the vulnerabilities or problems regarding satellite internet are presented. The majority of the solutions presented here were evaluated with the use of simulation in order to determine the effectiveness of the solution.

Yan et al. [51] proposed a cross-layer anti-jamming method in satellite internet. The proposed method uses a combination of the physical layer and network layer

approaches to effectively counteract jamming attacks on satellite links. The physical layer approach utilizes adaptive modulation and coding schemes to adjust the transmission rate based on the channel condition. The network layer approach uses a distributed anti-jamming algorithm to detect and avoid jamming attacks.

Wang et al. [48] presented Aerial Assistant, a system designed to safeguard ground-to-satellite communication networks. The proposed system utilizes unmanned aerial vehicles to provide a mobile communication platform that can act as a backup link in case of satellite signal loss or jamming attacks. The system uses software-defined radios on unmanned aerial vehicles to establish a communication link with ground stations and satellites, and can also be used to relay signals between different ground stations.

Nguyen and Chang [31] proposed a bio-metric-based authenticated key agreement protocol for user-to-user communications in mobile satellite networks. The proposed protocol uses bio-metric features such as fingerprints to authenticate users and establish a secure communication link between them. The protocol also utilizes public key encryption and digital signatures to provide confidentiality and integrity for the transmitted data.

Abdelsalam et al. [1] presented a robust security framework for Digital Video Broadcasting - Return Channel via Satellite (DVB-RCS) networks. The proposed framework uses a combination of cryptographic algorithms, digital signatures, and access control mechanisms to provide secure communication between different network entities. The proposed framework also includes a security management system that can detect and respond to security threats in real-time.

Lehto et al. [22] presented a protection evaluation framework for tactical satellite communication architectures. The proposed framework uses a comprehensive set of protection measures, including authentication, access control, encryption, and intrusion detection, to ensure the security of tactical satellite communication architectures. The proposed framework also includes a protection evaluation methodology that can be used to assess the effectiveness of the protection measures and identify any vulnerabilities in the system.

Bejarano et al. [35] investigated the security aspects of integrating communication security and transmission security in Internet Protocol (IP) satellite networks. The proposed approach uses a combination of encryption, authentication, and key management techniques to provide secure communication in IP satellite networks. The proposed approach also includes a threat analysis methodology that can be used to identify potential security vulnerabilities and threats in the system.

Caini et al. [8] introduced the concept of Delay- and Disruption-Tolerant Networking (DTN) as an alternative solution for future satellite networking applications. The proposed approach uses a store-and-forward mechanism to overcome the limitations of traditional network architectures, such as long delay times and frequent disruptions, which are common in satellite networks. The authors discussed the benefits of using DTN in satellite networks, including increased network resilience, improved data delivery rates, and reduced end-to-end delay. The study also presents a detailed overview of the DTN architecture, including its building blocks and protocols.

Several frameworks for risk assessment also exist, although these do not specialize in satellite internet or high-risk areas. Examples of this would be the *Threat Assessment and Remediation Analysis* (TARA) developed by MITRE [29], and *The*

Risk Management Framework (RMF) developed by NIST [30] (National Institute of Standards and Technology). These frameworks are developed for organizations to use in their risk management process and they present a method to identify risks, but they require certain knowledge that the intended user of our work is not expected to have.

3.4 Literature research gap

A common thread among the aforementioned related work is that they do not take high-risk areas into account, which could lead to some threats not being included in their result. By setting the scope of this work on high-risk areas, as well as targeting non-technical users, additional threats can be uncovered and relayed to users in a easy to understand manner.

Chapter 4

Method

Two research methods have been used in this thesis, a Structured Literature Review (SLR) as well as a Semi-Structured Interview. These methods were conducted in parallel to each other so that any findings in either method could be used to improve the other. However, while the findings in the SLR was used to improve the questions for the interviews, the results of the interviews were received to late to improve the search string used in the SLR. A literature review was chosen as this allowed us to gather data from the academic area and analyze what challenges have been found with satellite communication. By compiling data from multiple research papers we got a clear view of what threats these types of systems face.

An alternative to the literature review would be to investigate how we could attack satellite systems by conducting an experiment ourselves, this would also allow us to gather data on the threats to satellite systems but this poses some problems. The first problem is that we do not have access to these types of systems. The second problem is that we would not have access to the equipment required to perform the attacks already found in the pre-study. This work is focused on using satellite internet in a high-risk zone, this means that potential adversaries are nation-states that have access to a considerable amount of resources and equipment which would not be available to us and therefore not reflected in the final result.

4.1 Structured literature review

The Structured Literature Review (SLR) defined in [18] is the first method that was used to reach the aim of this work described in Section 1.1. This method was chosen over Systematic Literature Review since according to Karolinska Institutet University library [19], a Systematic Literature Review takes approximately 6 months up to 2 years. Since we had approximately 13 weeks to finish the work this was not time that was available to us. A structured literature review also differs from a systematic literature review in several aspects. In a structured review, the level of rigor and formalization is generally reduced compared to a systematic review. Some key differences include the absence of a predefined protocol, which guides the entire systematic review process. The search strategy in a structured review may be less extensive and systematic, with a focus on a limited number of databases or narrower search terms. The selection criteria may be less explicitly defined or more flexible, allowing for a wider range of studies to be included. The assessment of study quality may be less emphasized or omitted altogether in a structured review. Data extraction and synthesis may be less standardized and comprehensive, potentially

resulting in less rigorous analysis. Finally, structured reviews may not adhere to specific reporting guidelines, leading to potentially less standardized reporting. This was the reason the choice of a Structured Literature Review was chosen since this is similar but removes some of the steps of a Systematic Literature Review, allowing us to complete it within the time frame.

Previous research has been done on the vulnerabilities, threats, and shortcomings of satellite communication and by using the SLR method we could gather the information needed to answer our research questions. In Figure 4.1 the processes for both methods are visualized and the processes for SLR were as follows:

- Designing
  - **Select which databases should be used to extract the articles from** - The initial set of databases considered were *BTH Summon*[1], *IEEE Xplore*[2], and *Scopus*[3]. When searching in these databases we saw that BTH Summon did not produce any unique relevant results not found when searching in Scopus, and IEEE Xplore produced an overwhelming amount of results. This led to us choosing Scopus as our database. Scopus is a meta-database that presented results from multiple different other databases by only searching in the article metadata.
  - **Formulate a search string** - In this step, we collected keywords from articles that had been deemed relevant during our pre-study. We then used these keywords to create search blocks and find other relevant articles which we could use to extract other keywords and refine our search.
  - **Create criteria to use when determining article relevancy** - The criteria used for our initial selection of articles were:
    * Peer-reviewed, published in a journal or conference proceeding.
    * Written and published in English.
    * Published between 2003 and 2023.
    * Not a duplicate
    * Title or abstract mentions vulnerabilities or general security related to satellites.
  - **Design data extraction form** - From our stated research questions we defined the data to be extracted as:
    * Meta-Data:
      · Title
      · Publication year
      · Author(s)
      · Publication
      · DOI
    * Aim-specific data:

[1]https://bibliotek.bth.se/databases/44
[2]https://ieeexplore.ieee.org/Xplore/home.jsp
[3]https://www.scopus.com/home.uri

- Summary of vulnerabilities, threats, and where in the infrastructure it is located(Ground station, satellite, communication link, modem, etc) if stated.
- Risks mentioned in the article.
- Mitigations to the risks or threats if stated.
- Results of the paper if relevant.
- Technical know-how and/or resources required for exploiting the vulnerability if stated.

- Search
  - **Identify relevant articles based on title and abstract** - In this step, the search string was used to search in Scopus and then our criteria for relevancy were applied to determine if a full read-through was necessary. If we found it hard to decide the relevancy based on the title and abstract and the article fulfilled our other criteria, we included it in the articles selected for full-read-through.
  - **Include/exclude articles based on relevancy from full read-through** - In this step, all the articles deemed relevant from the previous step were read for a final decision on relevancy. To be determined relevant they had to contain information relevant to our aim-specific data in the data extraction form.

- Quality assessment and data extraction
  - **Assess the quality of the remaining articles** - Was the method used in the article sound and does the conclusion match the result?
  - **Extract data using the previously designed forms** - In this step all relevant articles were read and the data extraction form was filled in.

- Analyze
  - **Synthesize findings** - Here the data we extracted was analyzed using the threats and risk analysis that is discussed in Section 4.3.

4.1.1 Search string

When creating our search string we collected keywords from articles we had deemed relevant and evaluated them by including them in a search to see how they affected the result. As an example GPS signals are out of our scope which meant at first we excluded articles containing it. However this only excluded around 70 articles in the final search, and since it would be possible these articles contained some information relevant to us we opted to not exclude GPS from our search. Our search blocks below which were used to create the final search string provided a broader search in Scopus. However, considering that our topic seems to be facing a lot of innovation and development, a broader search was preferred to increase the likelihood of finding relevant articles. The search blocks were connected using AND in the searches.

- (satellite OR satcom)
- (security OR cybersecurity)
- (risk OR vulnerability OR threat OR exploit)
- (internet OR broadband OR communication)

4.2 Interviews

Semi-structured interviews were the other method used to reach the aim which is a hybrid between structured and unstructured interviews. This was chosen as the number of interviewees was estimated to be small enough that structured interviews would probably not produce significant results, and unstructured interviews would require the interviewer to have a deeper knowledge of the topic of the interview, as well as be an experienced interviewer which we were not. A structured interview consists only of pre-written questions and is a useful for when a high amount of participants is expected in the interviews. Unstructured interviews are more fluid and qualitative in nature, requiring an interviewer with experience both in interviewing, and the topic of the interview. A semi-structured interviews combines these methods into both pre-written questions, and allowing the interviewer to ask follow-up questions based on the participants answer.

During our pre-study, we saw that most of the academic research which was relevant to our topic was published either in the late 2000s or the last four years. This indicated to us that satellite internet is an area that has recently received a lot of attention, and the progress which is being made now may not yet be reflected in the academic literature. Interviews allowed us to get an insight into the experience of people working in the field of satellites, and people who have used satellite internet.

To identify companies we could interview we received help from our external supervisors at Knowit and CRD, as well as searching on the internet. To get in touch with people who have used satellite internet in a high-risk zone we received help from faculty members at BTH.

The participants of the interviews had three different backgrounds. We had one group of people who have used satellite internet in a high-risk areas, one group of people who work in the satellite development industry, and one group of people who work in the private security business. These groups presented different perspectives and knowledge of the area which we believed was valuable to us to answer our research questions and reach our aim.

When a company or person had agreed to participate in an interview we sent out the questions as well as possible time slots for them to choose from. The questions were sent out beforehand to allow the participants to read through and familiarize themselves with the questions, and ensure that if there were any questions the participant was unsure of, they had ample time to look this up.

For the structure of the questions we aimed at between 6 to 8 questions with possible sub-questions, and the semi-structured interview allowed us to ask follow-up questions to the answers given. The phases of the interview method were:

- Designing
  - **Secure participants** - In this step we reached out to our advisors, problem owners, faculty members of BTH, and several companies to ensure we have a large enough sample of individuals to interview.
  - **Identify interview subject and prepare questions** - Here we identified what minimum possible knowledge of satellite internet each group could be assumed to possess, and from this, we created a series of questions.
- Interviews
  - **Perform the interviews** - The participants we secured in the former step were interviewed.
- Analyzing data
  - **Analyze the answers** - Any threats, mitigations, or vulnerabilities discussed by the participant were extracted from the transcription.
  - **If any answers are unclear, revise the answers with the participant** - When the interview had been transcribed and anonymized the participant received a copy of it to approve for publishing along with any questions that arose during transcription.

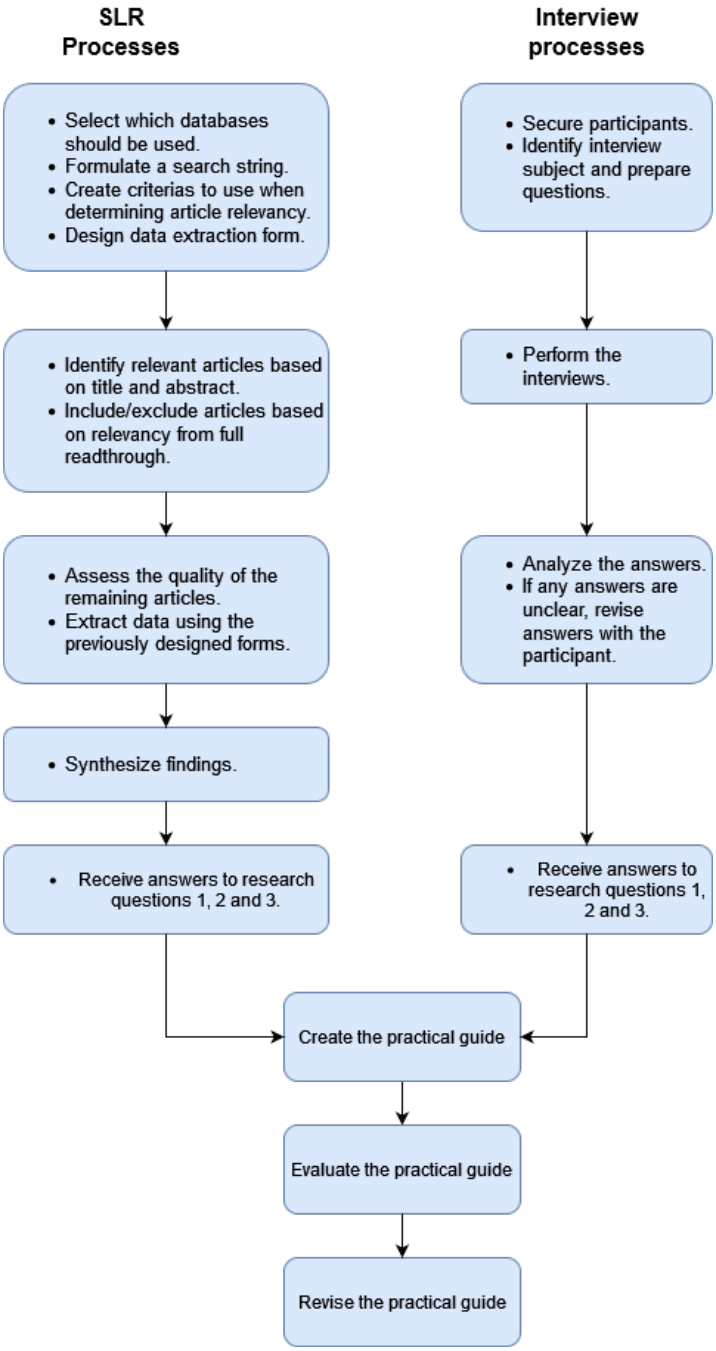

Figure 4.1: The steps and their order for the methods used.

4.2.1 Questions

From the interviewee groups previously identified which are satellite internet users in high-risk areas, satellite development companies, and private security companies, we created some base questions for each group which we could then use to create actual questions for the interviews. The base questions were derived from our research questions as well as additional information which could help reach our aim. This allowed us to tie the actual interview questions to our research questions, as well as identify and ask questions that overlapped with the different groups. This also

presented us with answers to similar questions from different perspectives and from interviewees with varying knowledge.

The base questions for each group were:

- Satellite internet users in high-risk areas
  - What, if any, guidelines did the users receive concerning security and what was the source of these guidelines?
  - Are they using any sort of security measures such as VPN or encrypting all emails?
  - What is their experience with using satellite internet as a connection?
  - How are they using the connection?
- Satellite development companies
  - What vulnerabilities are there in a satellite system?
  - What are their opinions on these vulnerabilities?
  - From a security perspective, what advancements have been made in recent years?
  - From a security perspective, which area has seen the least advancements in recent years?
  - From a security perspective, which area will see the most advancements in the coming years?
- Private security companies
  - Important risks discovered relating to satellite security?
  - What assumptions to make about a possible adversary?
  - What are their thoughts on satellite internet in a warzone?
  - Results of any risk analysis or assessment?

Using these base questions to identify the information we wanted, we created the interview questions for each group which can be found in Appendix A

4.3 Threat categorization, Risk assessment, and the confidentiality integrity and availability triad

In this section we present the different methods that were used to analyze our findings in the SLR and interviews, as well as discuss what other methods could have been used, and why we decided to not use them.

4.3.1 Threat categorization

To analyze the threats found during the SLR and interviews we decided to take a structured approach. This means we wanted to categorize the threats by using an established categorization. For this, we looked at the different threat modeling techniques to evaluate if they fit our purpose. We evaluated Process for Attack Simulation and Threat Analysis (PASTA) [47] but found that it contained a lot of activities we do not need, and it also does not contain an established categorization we could use for our purpose. We also evaluated Common Vulnerability Scoring System (CVSS) [43] but found that while this method would provide scoring for each threat it would not provide much else in terms of categorizing.

In the end, the threat modeling technique we chose was STRIDE [28]. This is more specifically a threat categorization that we could use to structure the threats found during the SLR and interviews. While STRIDE usually follows an application decomposition to identify and categorize threats, we skipped the application decomposition as there are many unknowns in the satellite internet infrastructure. Satellite internet providers use proprietary protocols of which the attributes are unknown to us, as well as possible differing structures of the network. Therefore we chose to only use STRIDE as a way to categorize the found threats, as we are not evaluating a specific provider in this work and we are gathering threats through the SLR and interviews.

STRIDE is a mnemonic that stands for:

- **S**poofing - Type of threat in which an adversary assumes the identity of another entity within the system.
- **T**ampering - Type of threat in which an adversary manipulates data in transit.
- **R**epudiation - Type of threat in which an adversary performs an unwanted action within the system that cannot be traced back to them.
- **I**nformation-disclosure - Type of threat in which an adversary gains unwanted access to data not meant for them.
- **D**enial-of-service - Type of threat in which an adversary is able to deny other users access to the system.
- **E**levation-of-privilege - Type of threat in which an adversary is able to gain privileges within the system not normally granted to them.

4.3.2 Risk assessment

We also choose to rank the risks found during this work. Assessing and ranking risks can be highly subjective as different people experience the impact of risks in different ways. Considering that the intended users of the produced document may not have prior knowledge of assessing risks, we believe a risk assessment where we describe the risks and motivate our scoring can be beneficial to them when evaluating these risks for themselves.

We believe that the generic risk model defined as $Riskscore = Probability * Impact$ fits our purpose. This model is known as a Probability Impact Matrix [11]. While this is a very simple way of assessing risks it is also easy to understand in an intuitive way for someone who may not be experienced in risk assessment. Using this calculation along with motivations for the probability and impact of each threat will provide an easy-to-understand risk assessment.

For the risk assessment we base the scores on a fictional scenario where assumptions are made about a fictional user of satellite internet in a high-risk area. This scenario is presented along with the scores in Section 5.3.2.

4.3.3 The confidentiality, integrity and availability triad

The Confidentiality, Integrity and Availability (CIA) triad is a model in information security which provides three key attributes which can be used to evaluate the security of information systems [20]. For our work, it was used to highlight how the threats we found affect the satellite system, and by extension improve the understanding of their impact for anyone reading the practical guide.

Figure 4.2: The CIA model with each key attribute.

In Figure 4.2 the CIA triad is presented as it is usually depicted, with each key attribute in the corners of the triangle and the lock in the middle representing the security of the information.

Confidentiality in this case is defined as information only being accessible to authorized parties who are supposed to have access to the information. Confidentiality can be ensured through the encryption of the data.

Integrity is defined as the trustworthiness of the information. Information is not changed in transit or otherwise tampered with. By using hashing algorithms or logging changes made to data this attribute can be met.

Availability is defined as authorized parties having access to the information they should have access to at all times. This could be realized by for example backing up the data or otherwise securing the uptime of a network.

4.4 Creating and evaluating the practical guide

In this section we present the practical guide which is the culmination of this work. We also present how the evaluation of it was performed.

4.4.1 Creating the practical guide

With the results yielded from the threat categorization and risk assessment as well as the mitigations found in the research material, the creation of the practical guide could begin. The guide was created in a document separate from this thesis; the document's final version can be found in Appendix C. The relevant results were compressed down into a form that was intended to be more easily understood and digestible by the intended users of the guide. The guide provides an introduction to satellite internet, a summary of the threat categorization and risk assessment, and a recommendation for mitigations and best practices for the secure use of satellite internet technology, based on the findings in our research.

4.4.2 Evaluating the practical guide

To evaluate the proposed practical guide we received help from Civil Rights Defenders to conduct a workshop where the participants were also employees of CRD. This workshop aimed to receive feedback from people who may not possess a lot of knowledge regarding security or information technology, as well as feedback from CRD, being an organization that could potentially benefit from the document. This feedback was important for creating a final document that could be useful for the intended users. The aspects of the document that we wanted to get feedback on were:

- **The technical level -** Is the guide on a good technical level for the intended users, is it understandable without getting too technical?
- **Language -** Is the guide written in a way that is comprehensible and grammatically correct?
- **Graphical illustrations -** Does the guide provide sufficient graphical illustrations on its different subjects to make it comprehensible?
- **Usability -** Is the guide usable for the intended users in its current state?
- **Unnecessary or missing information -** Is there any crucial information missing or any information that can be deemed as unnecessary and be removed?
- **Discuss the content -** Further discussions about the content of the practical guide.

With the resulting feedback gathered from the workshop, the practical guide will be revised with the feedback in mind to produce the final version of the document.

Chapter 5

Results

In this chapter we present the findings that were made during the SLR and interviews, as well as the analysis of the threats that were found. The structure of the practical guide along with the result of its evaluation is also presented.

5.1 Structured literature review

This section presents the results of the SLR. Using the final search string presented in Section 4.1.1 and the Scopus database as stated in Section 4.1, we received 457 search results. Table 5.1 shows the number of articles included based on relevancy.

	Scopus
Initial search	457
Relevant based on title and abstract	78
Relevant based on full read-through	25

Table 5.1: The number of articles during each phase of the SLR.

Table 5.1 shows that the first phase deemed $457 - 78 = 379$ articles irrelevant to our work, representing $\approx 83\%$ of the starting set of articles. The second phase removed 53 articles, $\approx 68\%$, from the second set of articles. This left 25 articles for the data extraction phase of the SLR.

5.1.1 Data extraction

From the final set of articles, we extracted data to answer our research questions:

- Vulnerabilities and what part of the network they affect. (*RQ1*)
- Threats and risks resulting from these vulnerabilities. (*RQ1/RQ2*)
- Methods for mitigating risks. (*RQ3*)

as well as the results of the paper if they were relevant to our work.

In Table 5.2 an overview is shown of what vulnerabilities were discussed by the authors in the papers. There were only 7 articles in which the authors discussed

different vulnerabilities. The majority of the articles had a focus on the different threats to satellite communication instead of the vulnerabilities, which in practice means that the authors often discussed ways to exploit different vulnerabilities instead of the vulnerabilities themselves.

Of the vulnerabilities, "weak or no encryption" and "weak authentication" are the two most mentioned vulnerabilities. These vulnerabilities arise from the limited resources available onboard satellites. Since satellite developers often need to make a compromise between security and the main mission capabilities of the satellite due to economic and physical restrictions, it becomes an economical decision to not equip the satellites with hardware that has enough computing power to perform secure encryption or authentication mechanisms without sacrificing the performance of the internet connection. Compare this to the terrestrial internet, where this problem does not exist [32, 36]. Insecure protocols are also a vulnerability mentioned, and this is due to the differences between satellite and terrestrial internet making some protocols undesirable when used in satellite communication. The use of traditional IPs like TCP in satellite communications, while still used, is proving difficult since it is not a secure protocol in itself but instead security is added on using various techniques such as TLS or IPsec. However in satellite communication these have the consequence of lowering data transfer rates and increasing latency. There is currently no solution to this issue, but it is being researched [13, 35]. Poor physical security refers to the satellite infrastructure being vulnerable to sabotage via an adversary gaining access to a ground station, space debris, or signal interference. Inadequate network segmentation is only mentioned in one article and refers to the satellite network being poorly segmented which could allow an adversary who gained elevated privileges to move laterally within the network to compromise more entities. The linkability vulnerability is also only mentioned in one article and refers to an adversary being able to link together different messages in the communication network.

Reference	Weak or no encryption	Weak authentication	Insecure protocols	Linkability	Poor physical security
[13]		✓	✓		
[26]	✓	✓			
[32]	✓	✓	✓		✓
[33]	✓		✓		
[35]	✓	✓	✓		✓
[50]	✓	✓		✓	
[10]	✓	✓			

Table 5.2: The vulnerabilities extracted during the SLR, with the vulnerabilities at the top and the references they were extracted from in the leftmost column.

Table 5.3 shows an overview of threats found, within our scope, during the SLR. In total the articles discussed 6 different threats to satellite communication. We can see that the most mentioned threat is eavesdropping, with 20 articles discussing it, which means that an adversary can gain access to the data being sent via satellite communication. Jamming is mentioned in 14 different articles and it entails an adversary using a strong physical signal to interfere with the communication link between the satellite and another entity, resulting in a loss of communication. Replay attacks are mentioned in 9 different articles and it means an adversary recording a

message sent by another entity and resending it at a later time. Message modification is mentioned in 11 articles, and this attack entails an adversary intercepting and modifying a message which was sent by another user. Malware is mentioned in 8 articles and it entails an adversary infecting an entity within the network with malicious software. Hijacking is mentioned in 5 different articles, and it means an adversary gaining control of a part of the network, this could for example be the satellite.

Reference	Eavesdropping	Replay attack	Jamming	Malware	Hijacking	Message modification
[1]	✓	✓				✓
[6]	✓	✓				
[7]	✓	✓	✓			✓
[8]	✓					✓
[10]	✓					✓
[12]			✓			
[13]	✓		✓	✓		
[14]	✓		✓			✓
[17]	✓		✓			
[22]			✓	✓		
[24]	✓	✓	✓	✓		✓
[25]	✓		✓			✓
[26]	✓			✓	✓	
[31]	✓	✓			✓	
[32]	✓		✓			✓
[33]	✓					
[35]	✓		✓		✓	✓
[38]					✓	
[39]				✓		
[40]	✓	✓	✓	✓		✓
[42]	✓	✓	✓	✓	✓	
[48]	✓					
[50]	✓	✓	✓			
[51]			✓			
[52]	✓	✓		✓		✓

Table 5.3: An overview of which threats were found in the articles deemed relevant in the SLR, with the threats on the top row and the reference they were extracted from in the leftmost column.

In Table 5.4 an overview of the mitigations extracted from the articles are shown. These are mitigations that users themselves can implement to secure their connection, without relying on the service provider to implement them. Any mitigations which could only be implemented by a service provider are not shown in this table as these would be out of the scope of this work.

Encryption is a mitigation that many of the articles discuss. This mitigation entails encrypting the data while in transit using techniques traditionally utilized in terrestrial internet connections. An example of this is end-to-end encryption in the form of a virtual private network.

User awareness is only mentioned in one article and it means educating users

Mitigation	Reference	Threat mitigated
Encryption	[10], [25], [26], [31], [32], [33], [35], [39], [40]	Eavesdropping, Replay attack, Message modification, Hijacking
User awareness	[39]	Eavesdropping, Jamming, Replay attack, Message modification, Malware, Hijacking
Software updates	[39]	Malware

Table 5.4: The mitigations found that a user can implement, which article mentions it, and what threat they affect.

about the potential security risks related to using satellite internet. This means educating them about the threats that exist and what they can do to mitigate these.

Software updates are also only mentioned in one article and it entails keeping all software up to date, to ensure that any vulnerabilities that are discovered and fixed by the developers are applied to the user's system.

5.2 Interviews

The anonymized transcriptions of the interviews can be found in Appendix B. At the start of each interview, the participants were made aware that any identifying information would be removed from the transcripts. They were also asked for consent on recording the interview for transcription purposes. After the interview the answers were transcribed, anonymized, and sent back to participants to be able to revise any answers and approve the transcription for inclusion in our work.

For interview 1 (Appendix B.1.1) and interview 3 (Appendix B.2.1) consent was granted to record but for interview 2 (Appendix B.1.2) consent was not granted. This meant that during interview 2, notes were taken instead. The answers to interview 2 were subsequently formatted and sent back to the participant to allow them to clarify or add to answers given during the interview, as well as approve them for publishing.

In interviews 1 and 2 the participants were from companies working with private security, and in interview 3 the participant was from a company working with security and engineering in the context of satellite communication.

From the interviews we mostly got confirmations of the vulnerabilities and threats found during the SLR, but another threat was discussed during the interviews with the private security companies when utilizing a satellite connection. Tracking is a threat that can be performed by an adversary triangulating the radio signals of the user segment, more commonly known as Radio Direction Finding [37, 41]. The end goal is to acquire the location of the user utilizing the satellite connection.

Concerning the first group of participants, satellite users in a high-risk area, we were not able to secure any interviews. We were able to send out the interview questions and receive answers from one person, but the answers were received as a questionnaire instead of a live interview. These answers can be found in Appendix B.3.

Concerning mitigations discussed by the interview participants, they discussed using encryption to secure the connection, but there was a larger emphasis on user awareness when using satellite systems. Being aware of what the threats are and using the system responsibly.

5.3 Threat categorization, risk assessment, and threats in relation to the CIA-triad

In this section, we present a categorization of the threats discovered in the SLR and interviews. We will also present a risk assessment made from a possible scenario in a high-risk zone, and also how the threats relate to the different attributes of the CIA-triad

5.3.1 Threat categorization

The threats found during the SLR and interviews were analyzed to determine what attack vectors they could use, after which the threats were categorized using STRIDE.

- **Communication Link**
  - Spoofing
    - Replay attack
      An attacker records a message and later resends the message. This could lead to an attacker being able to impersonate a real user.
  - Tampering
    - Message modification
      By eavesdropping on the communication link an attacker could read and alter a message, and by jamming the user's connection so it does not reach the satellite, the attacker could then send the modified message instead. The attacker could change messages to gain illegal access.
  - Repudiation
    - Replay attack
      An attacker records a message and later resends the same message. This could lead to unwanted actions such as an attacker impersonating a user and taking actions on their behalf.
    - Message modification
      By eavesdropping on the communication link an attacker could read and alter a message, and by jamming the user's connection so it does not reach the satellite, the attacker could then send the modified message instead. The attacker could take actions on behalf of the user which the user cannot deny as their message was used to perform these actions.
  - Information-Disclosure

    * Eavesdropping
      Using satellite signal capturing equipment in the form of a dish-antenna and software-defined radio receiver to intercept and collect sensitive information from people or organizations utilizing satellite internet. This leads to the disclosure of sensitive information and data due to the transmission channel not being secure and allowing for eavesdropping.
    * Tracking
      When a user is utilizing their satellite internet connection they are visible to potential parties looking for satellite communication signals in the area. This can, in turn, be used to determine the user's position. If a user is utilizing satellite internet in a potentially hostile area, the user may unintentionally make themselves a target of antagonistic forces interpreting their signal as an adversary trying to communicate. Additionally, a user may be tracked by government actors who seek to silence or incarcerate the user of the satellite internet connection.
  - DoS
    * Replay attack
      An attacker records a message and later resends the same message. The attacker could overflow the link by sending the same message over and over again to perform a DoS attack.
    * Jamming
      An attacker uses a jamming device to send interference signals degrading the connection between a ground device and the satellite. This could lead to the connection being dropped altogether.
  - Elevation-Of-Privilege
    * Message modification
      An attacker alters messages being sent. This could lead to an attacker gaining privileges they are not meant to have by for example altering the content of a control message.

- **Satellite**
  - Spoofing
    * Hijacking
      An attacker is able to hijack the satellite and control it. The attacker gains control of the satellite and evades detection to act as a legitimate node. The attacker is then able to read all data being sent via the satellite.
  - Tampering
    * Message modification
      If the attacker gains control of a satellite they could read and alter messages being sent through the satellite.
  - Repudiation

    - Replay attack
      An attacker records a message and later resends the same message. This could lead to the attacker making unwanted actions while impersonating someone, such as resending a control message sent by the ground station.
    - Message modification
      By hijacking the satellite the attacker could modify any message they want before sending it forward. The attacker could take actions on behalf of the user which the user cannot deny as their message was used to perform these actions.
  - DoS
    - Malware
      An attacker installs a malicious program on the satellite. If the satellite gets infected all connections with that satellite could be lost and it could fall out of orbit.
  - Elevation-Of-Privilege
    - Message modification
      An attacker alters messages being sent. This could lead to an attacker gaining privileges they are not meant to have by for example altering the content of a control message.

- **Ground station**
  - DoS
    - Malware
      An attacker manages to install a malicious program on a ground station. If the ground station is infected with malware the connection may be lost with the satellite.
  - Elevation-Of-Privilege
    - Message modification
      An attacker alters messages being sent. This could lead to an attacker gaining privileges they are not meant to have by for example altering the content of a control message.

- **User station**
  - DoS
    - Malware
      An attacker installs a malicious program on the user station. If the user station gets infected that user could lose their connection.

5.3.2 Risk assessment

The threats found were assessed by giving them a probability score and impact score, and then using a generic risk calculation of $Risk = Probability * Impact$ along with

explanations for the scores given, to let the readers of the guide understand the risks of using satellite internet. These scores and explanations are presented below. For probability and impact the score could range from 1 to 5, and the total score could therefore range from 1 $(1 * 1)$ to 25 $(5 * 5)$ for each threat.

For the risk assessment we need a scenario to estimate scores for the impact of the risks, as this is subjective. In this risk assessment we estimate the score based on a fictional civilian in a high-risk area such as a warzone. This civilian is a journalist and is currently reporting back to the headquarters on current events in the area. This means the civilian is most concerned with sending back information which they consider sensitive, as there may be a possibility of becoming a target of attack if a possible adversary does not wish for them to share the current events. They do not wish to be tracked in any way for concern of their own safety.

- **Hijacking**
  - Probability
    - Score: 1
    - Explanation:
      For an attacker to perform this action they need to access the satellite in some way. The most likely attack vector is the ground control station which then gives the attacker access to the satellite. However, the attacker needs intimate knowledge of the satellite architecture.
  - Impact
    - Score: 5
    - Explanation:
      The attacker is able to read and potentially modify all data being sent via the satellite. There is also a potential for the attacker to control the satellite and for example deorbit it.
  - Total score: 5
- **Jamming**
  - Probability
    - Score: 5
    - Explanation:
      Jamming devices can be very easily implemented and utilized by an attacker, due to the low complexity of implementation and deployment.
  - Impact
    - Score: 1
    - Explanation:
      This could lead to the connection being dropped altogether. This is however a temporary disruption and when the jamming device targets another frequency or is turned off, the connection is restored.
  - Total score: 5

- **Replay attack**
  - Probability
    - Score: 4
    - Explanation:
      An attacker needs to be able to record messages being sent as well as send them at a later time. This requires some technical know-how but its relative complexity is low.
  - Impact
    - Score: 2
    - Explanation:
      The impact depends on the message resent, but it could result in an attacker being able to impersonate a real user. This could lead to the disclosure of sensitive information and even the elevation of privilege for the attacker.
  - Total score: 8
- **Malware**
  - Probability
    - Score: 3
    - Explanation:
      The probability is medium here as there are known cases of malware infecting user terminals. The probability of ground stations being infected can also be considered relatively high as this is terrestrial communication. For the satellite to be infected by malware however would require specialized software and know-how which makes it relatively complex.
  - Impact
    - Score: 3
    - Explanation:
      If the ground station is infected with malware it is possible that the connection is lost with the satellite. If the satellite gets infected all connections with that satellite could be lost and it could fall out of orbit. If the user station gets infected that user could lose their connection.
  - Total score: 9
- **Eavesdropping**
  - Probability
    - Score: 5
    - Explanation:
      The probability of eavesdropping is high since it does not require too much knowledge of the satellite systems and fairly non-expensive equipment in order to be successful

  - Impact
    * Score: 2
    * Explanation:
      May lead to accidental disclosure of sensitive information and data due to the transmission channel not being secure and allowing for eavesdropping.
  - Total score: 10

- **Message modification**
  - Probability
    * Score: 3
    * Explanation:
      This requires the attacker to be able to intercept a message, alter the message and then resend the message to the receiver. The technical know-how involved is greater than that of a replay attack or simple eavesdropping since the attacker needs to be perceived as a legitimate user by the system.
  - Impact
    * Score: 4
    * Explanation:
      This could lead to an attacker gaining privileges they are not meant to have by for example altering the messages of a control message. The attacker could also take actions on behalf of the user which the user cannot deny as their message was used to perform these actions.
  - Total score: 12

- **Tracking**
  - Probability
    * Score: 4
    * Explanation:
      An adversary uses the communication link to locate satellite user stations. The complexity is not that high to realize this threat, and nation-states are known to have these capabilities and use them in high-risk zones.
  - Impact
    * Score: 5
    * Explanation:
      If a user is utilizing satellite internet in a potentially hostile area, the user may unintentionally make themselves a target of antagonistic forces interpreting their signal as an adversary trying to communicate. Additionally, a user may be tracked by government actors who seek to silence or incarcerate the user of the satellite internet connection.
  - Total score: 20

5.3.3 Threats in relation to the CIA-triad

In Figure 5.5 the threats that were found and what attribute of the CIA-triad they affect are presented. Hijacking, message modification, eavesdropping, malware, and tracking affect the confidentiality of the system. Replay attacks, hijacking, message modification, and malware affect the integrity of the system. Hijacking, jamming, and malware affect the availability of the system.

Threat	Confidentiality	Integrity	Availability
Replay attack		A replay attack can affect integrity by allowing attackers to replay old data and overwrite or manipulate current data, leading to the spreading of false or inaccurate information.	
Hijacking	Hijacking compromises confidentiality because attackers gain access to the communication channel and can intercept sensitive, confidential information.	Hijacking can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	Hijacking can impact availability by denying users access to critical resources. For example, if an attacker hijacks a communication channel during an emergency, it can prevent first responders from accessing important information.
Message-modification	Message modification compromises confidentiality because attackers can access and modify sensitive, confidential information.	Message modification can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	
Eavesdropping	Eavesdropping compromises confidentiality because attackers can intercept and access sensitive, confidential information.		
Jamming			Jamming can impact availability by blocking or disrupting the communication channels used by the satellite, thereby denying users access to critical resources during the use of the satellite systems.
Malware	Malware can compromise data confidentiality by potentially collecting and sending sensitive data to an attacker.	Malware can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	Malware can impact availability by causing delays in data transmission, affecting network performance, and potentially shutting down the system, which can have severe consequences in an emergency.
Tracking	Tracking can compromise the confidentiality of data, which can be particularly dangerous in a high-risk zone where sensitive information must be kept secure. It can expose the location of the users to the attackers, which can put them in danger.		

Table 5.5: The relation between the threats and Confidentiality, Integrity and Availability (CIA)

5.4 The practical guide and its evaluation

In this section, we present the structure and content of the resulting practical guide. The final version of the guide itself can be found in Appendix C. We also present the feedback received and corrections made after the practical guide had been reviewed through the workshop.

5.4.1 The practical guide

The resulting practical guide should be seen as a compressed and simplified version of the results in this thesis, aiming to gather the most important results and present them to the reader in a compact and comprehensible manner. The practical guide has the following chapter structure and content.

1. **Introduction** This is the first part of the practical guide in which we intended to provide some information about the document itself, what it is based on, its structure, and a disclaimer about its use and content.

    1.1 *About this project* - This section gives a small introduction to the project on which the practical guide is based and ties the document together with the thesis.

    1.2 *Structure of the guide* - This section gives an overview of the different chapters of the guide as well as some lines about each chapter of the document.

    1.3 *Scope and Disclaimer* - This section gives an insight into the scope of the entire project as well as a disclaimer providing some information on how the document is supposed to be used, what the content of the document is and why the content is written the way it is written.

2. **Satellite internet fundamentals** This chapter is the reader's first introduction to satellite internet in this document. This part is very similar to Chapter 2, the Background chapter of this thesis, although in the practical guide, it is slimmed down and simplified in order to be more comprehensive for the intended users.

    2.1 *Satellite internet infrastructure* - This section covers the different parts of the satellite network, also including an explanation of different satellite orbits.

    2.2 *Satellite vs Terrestrial internet* - This section shows a comparison between satellite internet and terrestrial internet, how they are different, similar, and tie into each other.

    2.3 *How the satellite internet system operates* - This section gives a small overview of how satellite internet networks operate, and how a common request would be handled.

3. **Common threats and risks** This chapter compiles all the threats and risks discovered throughout the project as well as what targets there are in the satellite network.

3.1 *Targets of attack* - This section explains the different targets in the satellite network.

3.2 *Threats and their consequences* - This section gives an overview of the different threats discovered through the SLR and interviews and gives a brief explanation of each of the threats as well as potential consequences should the threat become real.

4. **Risk assessment** This chapter presents a simple method of risk assessment that the reader can utilize after their own needs and situations. The chapter also presents an example risk assessment using the method described in this chapter performed by us the authors.

   4.1 *What is the perspective?* - This section presents a perspective of a user in a high-risk area and the following section will be the risk assessment done from this user's perspective and situation.

   4.2 *What are the risks?* - This section goes through each of the risks and gives them a ranking relating to probability and impact, as well as an explanation of the reasoning behind the score.

5. **Mitigations and best practices** This chapter presents the mitigations and best practices that a user should consider when using satellite internet in a high-risk area. These are also the results of the SLR and interviews performed throughout this project.

   5.1 *Mitigating the threats* - This section presents the different measures a user can take themselves in order to secure their communication.

   5.2 *Recommended best practices* - This section presents the best practices a user should consider in order to utilize their satellite internet equipment in as safe and secure a way as possible.

5.4.2 The workshop and evaluation of the practical guide

The workshop for evaluating the guide was performed with employees and associates of Civil Rights Defenders and took approximately three hours. The desired feedback questions found in Section 4.4.2 gave the following answers:

- **Q:** Is the guide on a good technical level for the intended user, is it understandable without getting too technical?
  A: The guide is in its current state on a technical level that is comprehensible for the users.

- **Q:** Is the guide written in a way that is comprehensible and grammatically correct?
  A: The guide is in its current state written in a comprehensible way, with some grammatical caveats needing correction.

- **Q:** Does the guide provide sufficient graphical illustrations on its different subjects in order to make it comprehensible?

A: The guide is in need of some further illustrations in order to be more comprehensive.

- **Q:** Is the guide usable for the chosen users in its current state?
  A: Yes it is usable, it could however need some clarifications in certain areas.
- **Q:** Is there any crucial information missing or is there any information that can be deemed as unnecessary and be removed?
  A: Nothing needs to be directly removed, some parts may need clarifying or adding content.

Here follows some of the most discussed and pressing feedback that was shared during the workshop. Whether the feedback was included or not and the reason for its inclusion or exclusion can be found in Section 6.4.

Possible additions:

- Capabilities that a country may have that can help determine the risks of using satellite internet, for example, how a risk compares in a warzone vs a dictatorship.
- Give more illustrations of satellite infrastructure.
- Do a comparison between devices.
- More specific ways to ensure secure usage (apps, protocols, etc).
- Put the mitigations into the risk sections.
- Expand best practices/mitigations, what risks do the mitigations apply to?
- Put some form of future work section in the practical guide.

Clarifications:

- Clarification on what devices are concerned by the document.
- Define the area the document targets or defines.
- Make sure the scope/disclaimer clarifies what the document is supposed to be used for.
- Make it clear that the user should apply their own risk assessment depending on their own situation and needs.
- Clarify that the user may utilize the scoring system for their own specific needs.

Chapter 6

Analysis and Discussion

In this chapter we present an analysis of the findings presented in Chapter 5, as well as a discussion on what these findings could mean. We discuss potential shortcomings in our approach and the feedback received during the evaluation of the practical guide. Finally we discuss the environmental, societal and ethical aspects of our work.

6.1 The literature review

6.1.1 The articles

When looking at the articles extracted through the SLR, as previously clarified in the description of Chapter 3, we decided to categorize them. These categories were studies and reviews that took a similar approach as the one we have used in this study, literature in which the method had included more practical and experimental approaches to achieve the results, and finally literature that proposed some form of a new solution to any problem that was related to satellite internet security.

The studies presented in Section 3.1 take similar approaches to data collection as this project has done through the SLR. Many vulnerabilities that have been documented are reoccurring throughout the different studies, such as jamming, eavesdropping, and DoS attacks. The context and scope of the studies differ in that some studies look at the satellite systems as a whole [3, 7, 23, 26, 39, 40, 42, 50], while others are targeting a more specific part of the system [17], a specific attack or threat [52], or a very specific type of satellite system [13, 14, 24]. However, the studies in Section 3.1 as well as the following ones do not share a part of the context of this thesis in that they do not consider the use of these systems in high-risk areas. That being said, the majority of vulnerabilities and threats, risks, and risk-mitigations discovered in these studies can be applied in a high-risk area as well.

The studies presented in Section 3.2 have shown that while some vulnerabilities and threats have been mitigated, others still pose a significant risk to satellite communication systems today. For example, the use of weak encryption algorithms, unsecured communication channels, and insufficient authentication mechanisms could still allow attackers to compromise satellite internet systems.

The studies presented in Section 3.3 have demonstrated that combining cryptographic techniques and other security mechanisms can effectively protect satellite communication systems.

6.1.2 The SLR findings

We found six vulnerabilities and six threats, but no mention of tracking as a threat in the research papers we extracted data from. This could be attributed to the scope of these research papers. The research papers we found were targeted at the satellite ISPs as they mostly provided solutions that they could implement. This is a valid target audience as with the service provider improving the security this also improves the security for the end user. However with the scope of this work focusing on how a user would be impacted by our findings, it provides a different perspective, and because tracking signals is not a threat specifically towards satellite communication, but a threat for all emitters generating some type of signal it may be that the authors chose not to mention it as it could possibly be out of their scope. The scope of this work being satellite internet usage in high-risk areas also presents a different view on the capabilities of an adversary. Parties of a conflict in a warzone can, and likely will, employ attacks against satellite communication in general which may be regarded as off-limits during peacetime.

We only presented three mitigations found during our SLR. While there were more in the research articles, the majority of the mitigations discussed would require the implementation to be made by the satellite ISP. It is also important to remember that the mitigations found were targeting the satellite communication specific threats, but it is still an extension of the internet, and as such best practices and mitigations for using internet in general still apply.

What we found when researching threats is also that different names were used for the same type of threat. An example of this is K.Shilling and A.Dmitrienko, which describe alternation attacks and defined this as an attacker altering transmitted data [40]. A.Abdelsalam et al. mention traffic hijacking as a type of attack threatening satellite networks, and defines this as an attack modifying messages in transit [1]. These attacks have the same results with similar definition but are named differently in the papers. This points to a lack of standardization when discussing threats to satellite networks, and highlights the importance of comparing the definitions when researching this area.

An important note is also that a majority of the research papers included in the SLR were from 2019 and onwards, which points to an increasing interest in research regarding satellite internet security. In interview three with the satellite company, the participant compared internet via satellite to the early stages of the terrestrial internet which implies that the more widespread its use becomes it may also become more attractive to future attackers, which could produce new threats to satellite internet not previously discovered by researchers.

6.2 The interviews

6.2.1 Relation to the SLR

As shown in the results, our SLR identified several vulnerabilities and threats associated with using satellite internet technology in a high-risk zone. Through interviews with the security and risk assessment companies as well as the experts in satellite security and engineering, we were able to confirm and expand on these findings.

The private security companies we interviewed confirmed that eavesdropping was a significant vulnerability associated with satellite internet technology in high-risk zones. They noted that intercepting data transmitted over satellite links was a common tactic used by malicious actors seeking to gain access to sensitive information.

The satellite expert we interviewed confirmed several other vulnerabilities and threats found during the literature study. Jamming and malware were confirmed as significant threats to the integrity and availability of satellite communication systems. Insecure protocols were also identified as a potential vulnerability that could be exploited by attackers seeking to gain unauthorized access to the system.

Interestingly, tracking a user's location was not a threat that we found to be extensively covered in our literature review. However, it emerged as one of the most discussed threats during our interviews with the private security companies. They highlighted that tracking the location of satellite users was a significant concern, particularly in high-risk zones where surveillance and monitoring activities were prevalent. They especially highlighted that this was something that Government-actors certainly has the capability to do. One of the reasons why tracking was not a threat in any of the studies could be that it is a threat towards radio waves in general, which may have been out of their scope.

6.2.2 Finding participants with different perspectives

Our goal with the three different groups of participants, the private security experts, the experts in satellite systems, and people who had used these satellite internet terminals in a high-risk area was to gain multiple perspectives on the vulnerabilities, threats, and risks associated with using satellite internet technology in high-risk zones, as well as to gain some useful insights into the use of these systems.

The first seven weeks of the study were partially used to rigorously send out requests for interview participants and the search for participants with a user perspective continued even into the final weeks of this study.

In total, we reached out to seventeen different organizations and experts for interviews. Among these, two were agencies, eleven were technical organizations or experts working with satellite internet and four were security companies dealing with risk assessment. Out of these we unfortunately only managed to secure interviews with two private security companies and one expert in satellite security and engineering.

We were also unfortunately only able to secure one participant from the group of people who had used satellite internet terminals in a high-risk area. The reason for this was that the people we were trying to get in contact with were people in Ukraine, both civilian and military, who had used satellite internet systems. But understandably due to the current situation in Ukraine, this proved difficult. We also believe that the questions we wrote can be intimidating outside of an interview. When we ask the questions we can explain any uncertainties to the participant, and reword the question if needed. When sending them out to possible participants who do not possess a lot of knowledge regarding information security or similar, it is possible they felt that they did not have any answers to our questions.

The questions we made were not designed as a questionnaire and therefore it is not surprising that the answers we received, from the user of satellite internet in a

high-risk zone, were short and often non-descriptive.

While it is arguable that we could have been more proactive in securing interview participants, the limited number of final participants we were able to interview still provided valuable insights and information. They also provided us with a unique threat that did not show up during our literature review.

6.3 Threat categorization, risk assessment, and inclusion of the CIA triad

In this section, the results of the threat categorization, risk assessment, and inclusion of the threats in relation to the CIA triad are analyzed and discussed.

6.3.1 Threats categorization

Regarding the threat categorization that was performed, it showed that the most exposed part of the satellite network segment is the communication link. Its wireless nature and being the target of attack for the most mentioned threats such as eavesdropping, replay attack, and jamming, this comes as no surprise. If an attacker wants to gain access to data in transit, this segment of the network is the least complex part to attack and therefore also the most attractive.

The satellite segment is mostly concerned with taking over the satellite in some way. If an attacker is able to hijack a satellite they could theoretically perform all of these attacks to negatively affect the user. While it seems more exposed to attacks than the ground segment, it is also important to note that it is relatively complex to attack it, and it would probably require a lot of resources and knowledge to successfully take over a satellite.

Regarding the ground station segment, this part of the network could be used by an attacker to negatively affect a user by either modifying their messages or infecting the segment with malware to cause DoS. While it seems less exposed than the satellite segment, the ground station has direct internet access. While terrestrial internet threats are out of the scope of this work they would still apply and could be used against this segment.

The only threat in the user station section is malware. This threat has been executed before and was the only threat in the literature we found that could apply to it. Not mentioned in the literature study is also gaining physical access to the user station which could allow an attacker to illegitimately modify it [49].

6.3.2 Risk assessment

Regarding the risks that were found these relate directly back to the threats and vulnerabilities. In our risk assessment, we chose to take a simpler approach to present the risks in a way that is easily understandable for the intended users of our guide. While we feel we succeeded in this regard we also failed to consider its utility. The risk assessment in this work was made from a specific scenario, and it becomes difficult to generalize and apply it for anything outside of the specified context that was considered. However performing a risk assessment that is general and can later

be applied by the reader was never the intent, and is something that could harm the purpose of the guide. A reader should only use it to get a first initial understanding of the risks of using satellite internet in high-risk zones, and if they believe the risks are manageable they should then perform their own risk assessment for their specific context.

6.3.3 Inclusion of the CIA triad

The CIA triad is a widely used model in information security that breaks down the main goals of information security into three categories: confidentiality, integrity, and availability. By relating threats to each of these categories, it provides a clear and simple perspective that can be easier to digest and understand.

By breaking down the threats into these three categories, the CIA triad provides a simplified perspective on the goals of information security and the threats that can compromise them. This is particularly useful for those who may not be familiar with the technical details of the threats, as it provides a clear and straightforward way of understanding the impact of these threats on the system.

Moreover, by using the CIA triad to analyze threats, it also helps to prioritize countermeasures to address these threats. For example, if a threat is identified as compromising confidentiality, then measures such as encryption and secure communication protocols can be prioritized to prevent unauthorized access to sensitive information.

6.4 Practical guide

In this section, we will analyze and discuss the resulting practical guide. We will discuss its perceived usability from the perspective of the CRD employees present during the evaluation workshop, the feedback we received, what made it into the final version of the practical guide, what did not, and why that is.

6.4.1 Usability

Based on the feedback received from the workshop participants, the practical guide was found to be a valuable resource for its intended users. The participants confirmed that the guide provided a good introduction to satellite-based internet and its most common threats and risks.

Additionally, the potential mitigations and best practices provided in the guide were seen as implementable and usable to manage the risks associated with using satellite internet, without getting too complicated.

The document was also accessible and understandable, even for people who did not have a background in computer science. The technical level of the guide was well received, and participants appreciated the explanations provided. The use of straightforward language and clear explanations were noted as strengths of the guide.

The intended purpose of the practical guide was to provide an initial overview of satellite-based internet and its associated risks and to aid individuals and orga-

nizations in making an informed decision about whether to use satellite internet in high-risk zones. Participants noted that the guide fulfilled this purpose well.

One suggestion for improvement was to condense the information provided in the guide into a list of just a couple of pages since the guide in its current state is quite extensive. This would make the information more accessible and easier to refer to for users. While the guide was well received overall, participants suggested that a shorter version of the document may be more useful in practice.

6.4.2 Feedback and revision

Overall, the usability of the practical guide was deemed to be satisfactory by workshop participants. They saw the document as a valuable resource for organizations and individuals considering the use of satellite internet in high-risk zones. The guide was accessible, and understandable, and provided valuable information on the risks associated with using satellite internet, as well as potential mitigations and best practices.

However, there was some feedback on the overall structure as well as some suggestions for improvement given by the participants of the workshop. The clarifications stated in Section 5.4.2 were all implemented as well as the suggested additions:

- Give more illustrations of satellite infrastructure.
- Expand best practices/mitigations, what risks do the mitigations apply to?

This was relevant feedback that was also still within the scope of the study. The feedback and suggestions that were not implemented during the revision of the practical guide and the reasoning for its exclusion are presented below.

- Capabilities that a country may have that can help determine the risks of using satellite internet, for example, how does the risk compare in a war zone vs a dictatorship?

  This feedback was excluded as it goes beyond the scope of the practical guide, which was focused on providing a general overview of the risks associated with using satellite internet in high-risk areas. Additionally, geopolitical factors such as the political climate and government capabilities may be constantly changing, making it difficult to provide concrete information.

- Do a comparison between devices.

  This feedback was excluded as it goes beyond the scope of the practical guide, which was focused on providing a general overview of the risks associated with using satellite internet in high-risk areas. Also, the majority of specific devices are using proprietary technology, meaning that it is hard to get clear specifics and compare functionality. Additionally, comparing specific devices may not be practical as new devices and technologies are constantly being developed.

- More specific ways to ensure secure usage (apps, protocols, etc).

This feedback was excluded as it goes beyond the scope of the practical guide, which was focused on providing a general overview of the risks associated with using satellite internet in high-risk areas. Additionally, providing specific recommendations on apps and protocols may be difficult as they may not be universally applicable and may require technical expertise to implement.

- Put some form of future work section in the practical guide.

  This feedback was excluded as the practical guide was designed to be a standalone resource that could be used immediately by its intended audience. We believe the future work section provides more relevance to the thesis since that is the work that the practical guide is built upon. Additionally, a future work section may not be practical as it may require ongoing updates and revisions to the practical guide.

- Put the mitigations into the risk sections.

  This feedback was excluded due to the structure of the document. Since the mitigations to the risks are presented in a later chapter, we believed it to be more relevant to associate the mitigations to the risks in the mitigations section of the practical guide. Here we tie together the risk to the relevant attributes of the CIA triad and the risks to their mitigations to give an overview of what has been discussed in the guide.

6.5 Validity threats

This study aimed to identify and analyze the security threats associated with satellite internet in high-risk areas and develop a practical guide for individuals and organizations considering its use. However, the validity of the study may have been influenced by several threats that need to be addressed.

- Although we conducted a SLR to identify relevant studies, the threats we found may not reflect the full range of risks associated with the use of satellite internet technology. As this work was limited in scope and because we discovered threats in the interviews which were not present in the literature study, there may be additional information or threats we may have missed. Snowballing was considered as a supplement to the SLR, however our initial trial of snowballing did not produce any additional findings and we therefore disregarded this method.

- While we attempted to obtain a diverse range of perspectives by interviewing individuals from private security companies, satellite companies, and people who have used satellite internet technology in high-risk zones, we were only able to interview two private security companies and one satellite company. Moreover, we were unable to secure any interviews with people who had used satellite internet technology in high-risk areas. While we were able to obtain some answers from a contact who had used these systems in Ukraine, the

answers to the interview questions were only provided in written form due to the contact not being able to participate in an interview. Since the questions were not designed to be answered as a questionnaire, the written answers were not very extensive, and could unfortunately not provide the perspective that was desired. These are all factors that may have limited the representativeness of our findings.

- In our threat analysis we used STRIDE to categorize the threats and identify their possible impacts. This only provides a shallow analysis of the threats and it is possible that creating a data-flow-diagram of the general satellite infrastructure, which we could then apply STRIDE, or other threat modeling techniques discussed in the method chapter, would produce more threats than we encountered in our literature study. However due to time constraints, and the practical guide we created only meant to provide an overview of threats targeting a user, we feel that our approach was sufficient.
- In addition, while we evaluated the practical guide with the assistance of employees of CRD, who have an insight into these areas, we were unable to test the practical guide in the field due to the scope and time constraints of our study. This may limit the validity of the guide, as the outcome of its use in real-world settings may differ.
- Lastly, the 13-week time constraints of our study may have limited the depth and breadth of our investigation. We acknowledge that a longer study could have potentially uncovered additional threats or provided more comprehensive and nuanced results. This would especially allow us to further investigate why tracking only showed up in the interviews.

Despite these limitations, we believe that our study provides valuable insights into the security threats associated with satellite internet in high-risk areas and offers practical recommendations for its use. We recommend future studies address these limitations by using multiple frameworks and obtaining a more diverse sample.

6.6 Ethical, societal and sustainability aspects

The ethical aspect of this work was to ensure the answers gathered in the interviews were anonymized before they were presented, to ensure the participants can not be identified and felt safe answering our questions. It was also important that we presented the limitations of this work in order to ensure that any organization or person that would utilize the Practical Guide, as a basis for their decision to use satellite internet in a high-risk area, is aware that the guide may be flawed in some way we have not been able to anticipate.

The societal aspect of this work has been its intention to aid people who work or live in high-risk areas. This work is intended to help in efforts to promote freedom and free speech which may lead to the betterment of communities in high-risk areas. The result of this project is also meant to be a resource for anyone that sees the potential of using satellite internet for safe communications when there is no terrestrial internet available.

The sustainability aspect of this work was providing organizations with a cost-effective guide that can help them make initial informed decisions about the use of satellite internet. If there are any factors in the guide that could make or break whether the decision is made to utilize satellite internet communication, organizations could save both time and resources that may be used in other areas of their work, thus promoting economic sustainability. Besides the cost savings, this guide also promotes environmental and social sustainability by providing guidelines on how this technology may be used safely and responsibly.

Chapter 7

Conclusions and Future Work

In this chapter, the answers to the research questions are presented, as well as suggestions for future work in the area of satellite internet usage in high-risk areas which could also provide improvements to the practical guide.

7.1 Conclusion

While a satellite internet connection is a great choice when availability of the internet connection is the main concern, in our work we discovered what threats face users of satellite internet in high- risk areas. The most surprising of these threats where tracking, otherwise known as radio direction finding, as this threat could have an impact on personal safety. While this requires further research, due to time constraints we were not able to investigate this threat on a deeper level.

The practical guide we created, containing the results of this work in a condensed manner, provides an overview of area of satellite internet security. When evaluated it was was considered to present the threats that exist, and what a user themselves can do to mitigate them, in an easy to understand manner.

The most important contributions of this work was the user awareness the practical guide creates, as well as discovering the threat of tracking. With these contributions, we can hopefully create a safer usage of satellite internet in high-risk areas.

7.1.1 RQ1

What vulnerabilities and threats exist that are related to any part of the satellite internet infrastructure that can have a negative impact on a user of satellite internet technology in a high-risk area?

The most prominent vulnerabilities found were that satellite internet often uses weak or no encryption, weak authentication, and insecure protocols in their infrastructure. Poor physical security was also a mentioned vulnerability which would translate into an adversary physically sabotaging part of the network. Linkability was a vulnerability that showed up both in the literature study and interviews, and it could potentially allow an adversary to link together different messages in the network. The last vulnerability found was inadequate network segmentation which could lead to an adversary being able to laterally move within the network and possibly gain additional access they should not have.

Weak or no encryption seems to have been a problem throughout the history of satellite internet, and it comes from the performance degradation it can produce in these networks. Considering that satellite internet already has had lower throughput, it seems like the choice to encrypt has been left to the users themselves. Weak authentication has also been a reoccurring vulnerability. The traditional insecure protocols that are used also makes them vulnerable to certain attacks, such as replay attack.

The threats we found during our research that target the satellite infrastructure and have a negative impact on a user, and which they can mitigate in some way were eavesdropping, jamming, tracking, replay attack, hijacking, message modification, and malware. Of these, jamming and tracking are physical threats that target the radio signals the terminal emits. Eavesdropping, replay attacks, and message modification target the communication link. Hijacking and malware target the physical devices in the infrastructure, such as the ground segment, satellite, or user segment.

7.1.2 RQ2

What are the risks of using satellite internet communication in a high-risk area that may come as a consequence of the vulnerabilities and threats found in satellite internet infrastructure?

From the threats in the answer to *RQ1*, in a high-risk area, jamming, eavesdropping, and tracking are the threats with the highest probability. Jamming only requires specialized equipment known as a jammer, and at least for warzones can be assumed to be in use by the parties in conflict. Eavesdropping can be performed by buying relatively cheap equipment and has been successfully performed by researchers in the past, which means an adversary with nation-state backing should be assumed to possess and utilize these capabilities. Concerning tracking, this threat also requires specialized equipment known to at least be available to nation-state actors and can be assumed to be in use in high-risk areas, which makes it all the more important for users to be aware of the possibility to be tracked.

Malware has been used before in a DoS attack against user terminals, showing that malware with this capability and the risk of being exposed to this type of threat exists.

Replay attack and message modification are similar in execution, with the difference being that message modification, as the name suggests, requires the original message to be modified in some way. Due to its lower complexity, the replay attack has a higher probability while message modification has a higher impact.

Hijacking is the threat with the highest relative complexity of all the threats found, as it involves gaining access to and controlling a satellite. This means it also has the lowest probability considering the resources it takes to successfully execute this attack.

7.1.3 RQ3

What measures can be taken by a user to mitigate the risks of using satellite internet in a high-risk area found in RQ2?

During our literature study, we found many solutions proposed by authors to either get rid of found vulnerabilities or mitigate threats. However, as the papers were not user-focused, many solutions found were not applicable in our case. An example solution was to use more secure protocols, but a user would not have any control over what protocols are used in the satellite system. In our interviews, all the participants talked about user awareness as important for using satellite internet responsibly. Therefore the mitigations we ended up with were encryption, user awareness, and software updates.

The most important of these mitigations, which is the main contribution of this work, is user awareness as it indirectly affects all the threats. If the user is aware of what threats they are faced with when using satellite internet, they are more likely to use it in a responsible way and for example not share sensitive information via a satellite connection.

Using some form of encryption was the most popular mitigation found in the literature study and it was no surprise considering the history of satellite providers sending data in cleartext. This mitigation showed up both as a service provider implementation and user implementation. Considering the experimental studies showing how relatively easy eavesdropping was to perform and eavesdropping being the most frequent threat, using encryption such as a virtual private network, or encrypting email when sending sensitive information becomes an important practice for anyone using satellite internet.

Keeping software security up to date on all devices is a common recommendation for terrestrial internet and it also applies to satellite internet. This mitigation although only mentioned in one article in the literature study and not in the interviews, is still an important mitigation that the user can apply to further secure their connection.

7.2 Future work

The practical guide in its current state provides a useful introduction to satellite-based internet, including its most common general risks and vulnerabilities. However, there is still much to be explored in this area, and potential future work could include:

- Exploring high-risk areas further. This could involve conducting additional interviews with people working in high-risk areas or organizations with clients working in high-risk areas to gain a better understanding of the specific risks and vulnerabilities they face. Furthermore, it could also be useful to explore what capabilities different parties have in high-risk areas.

- Conducting further investigation into the topic of radiowaves in relation to satellite internet. Our interviews with security and risk assessment companies suggested that tracking radio signals was a prevalent risk, yet this vulnerability was not mentioned in the literature we examined. Future research could examine this area in more detail to identify potential threats and mitigation strategies related to radio signals.

- Conducting a comparison between different satellite internet providers and their technology to compare functionality and services in terms of security.

This could require the acquisition of devices from several satellite ISPs and also interviews with these companies to gain a deeper understanding of their security measures and protocols.

- Analyzing and comparing different protocols, applications, and services for security that can be utilized by a satellite internet user in a high-risk area to optimize and ensure the safest possible usage. This could involve testing and evaluating different protocols and applications to identify the most effective and secure options for users in high-risk areas.

- Expand the scope of the guide to include law perspectives, both international and local. This could for example take into consideration the aspect of satellite internet providers who do not provide internet to certain countries or areas due to the local laws and regulations.

It should be noted that these potential improvements would require a scope that is significantly more extensive than that of our work. However, by exploring these areas further, we can gain a better understanding of the risks and vulnerabilities associated with satellite internet use in high-risk areas and provide more comprehensive guidance to users. Furthermore, because we found that the majority of relevant research had recently been conducted, this points to the area gaining a lot of attention which means conducting similar research to our work in a few years could produce more interesting results.

References

[1] A. Abdelsalam, D. Caragata, M. Luglio, C. Roseti, and F. Zampognaro, "Robust security framework for dvb-rcs satellite networks (rssn)," *International Journal of Satellite Communications and Networking*, vol. 35, no. 1, pp. 17–43, 2017. [Online]. Available: https://doi.org/10.1002/sat.1154

[2] A. Adelsbach and U. Greveler, "Satellite communication without privacy - attacker's paradise," in *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, 2005, pp. 257–268. [Online]. Available: https://www.researchgate.net/publication/221307186_Satellite_Communication_without_Privacy_-_Attacker's_Paradise

[3] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Hoyhtya, "Security of satellite-terrestrial communications: Challenges and potential solutions," *IEEE Access*, vol. 10, pp. 96 038–96 052, 2022.

[4] B. Al Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, B. Allen, and B. Moores, "Next generation mega satellite networks for access equality: Opportunities, challenges, and performance," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 18–24, 2022. [Online]. Available: https://doi.org/10.1109/MCOM.001.2100802

[5] Al Jazeera. (2022) Russia behind cyberattack against internet network in ukraine. [Accessed March 31, 2023]. [Online]. Available: https://www.aljazeera.com/news/2022/5/10/russia-behind-cyberattack-against-internet-network-in-ukraine

[6] G. Baselt, M. Strohmeier, J. Pavur, V. Lenders, and I. Martinovic, "Security and privacy issues of satellite communication in the aviation domain," in *International Conference on Cyber Conflict, CYCON*, vol. 2022-May, 2022, pp. 285–307. [Online]. Available: https://doi.org/10.23919/CyCon55549.2022.9811060

[7] M. Bradbury, C. Maple, H. Yuan, U. I. Atmaca, and S. Cannizzaro, "Identifying attack surfaces in the evolving space industry using reference architectures," in *IEEE Aerospace Conference Proceedings*, 2020. [Online]. Available: https://doi.org/10.1109/AERO47225.2020.9172785

[8] C. Caini, H. Cruickshank, S. Farrell, and M. Marchese, "Delay-and disruption-tolerant networking (dtn): An alternative solution for future satellite networking applications," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 1980–1997, 2011. [Online]. Available: https://doi.org/10.1109/JPROC.2011.2158378

[9] Civil Rights Defenders. Civil rights defenders: Vision, mission and work methods. [Accessed Jan. 16, 2023]. [Online]. Available: https://crd.org/working-methods/

[10] H. Cruickshank, L. Liangl, P. Pillai, M. Noisternig, B. Collini-Nocker, and G. Fairhurst, "Unified link layer security design for ip encapsulation using unidirectional lightweight encapsulation over satellites," in *IET Conference Publications*, 2009. [Online]. Available: https://doi.org/10.1049/cp.2009.1153

[11] V. Dumbravă and S. V. Iacob, "Using probability – impact matrix in analysis and risk assessment projects," *Journal of Knowledge Management, Economics, and Information Technology*, vol. 3, pp. 1–7, 2013.

[12] G. Giuliari, T. Ciussani, A. Perrig, and A. Singla, "Icarus: Attacking low earth orbit satellite networks," in *USENIX Annual Technical Conference*, 2021.

[13] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 1, pp. 53–87, 2022. [Online]. Available: https://doi.org/10.1109/COMST.2021.3131332

[14] D. He, X. Li, S. Chan, J. Gao, and M. Guizani, "Security analysis of a space-based wireless network," *IEEE Network*, vol. 33, no. 1, pp. 36–43, 2019. [Online]. Available: https://doi.org/10.1109/MNET.2018.1800194

[15] Y. Hu and V. Li, "Satellite-based internet: a tutorial," *IEEE Communications Magazine*, vol. 39, no. 3, pp. 154–162, 2001. [Online]. Available: https://doi.org/10.1109/35.910603

[16] M. K. Iqbal, M. B. Iqbal, S. Shamoon, and M. Bhatti, "Future of satellite broadband internet services and comparison with terrestrial access methods e.g. dsl and cable modem," in *2013 3rd IEEE International Conference on Computer, Control and Communication (IC4)*, 2013, pp. 1–5. [Online]. Available: https://doi.org/10.1109/IC4.2013.6653763

[17] G. Jang, B. You, and H. Jung, "A survey on physical layer security schemes in satellite networks," in *International Conference on ICT Convergence*, vol. 2022-October, 2022, pp. 1213–1215. [Online]. Available: https://doi.org/10.1109/ICTC55196.2022.9952733

[18] Karolinska Institutet University Library. (2023) Structured literature review. [Accessed Feb. 3, 2023]. [Online]. Available: https://kib.ki.se/en/search-evaluate/systematic-reviews/structured-literature-reviews-guide-students

[19] ——. (2023) Systematic reviews. [Accessed Feb. 3, 2023]. [Online]. Available: https://kib.ki.se/en/search-evaluate/systematic-reviews

[20] C. Kidd. (2023) Is the cia triad relevant? confidentiality, integrity & availability today. [Accessed April 23, 2023]. [Online]. Available: https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html

[21] K. Kravchenko. (2021) Ukraine shows promise and peril of satellite internet in war zones. [Accessed March

31, 2023]. [Online]. Available: https://www.devex.com/news/ukraine-shows-promise-and-peril-of-satellite-internet-in-war-zones-102794

[22] G. M. Lehto, G. Edlund, T. Smigla, and F. Afinidad, "Protection evaluation framework for tactical satcom architectures," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2013, pp. 1008–1013. [Online]. Available: https://doi.org/10.1109/MILCOM.2013.175

[23] S. Lohani and R. Joshi, "Satellite network security," in *Proceedings - 2020 International Conference on Emerging Trends in Communication, Control and Computing, ICONC3 2020*, 2020.

[24] Y. Ma, D. Yang, D. Zhang, H. Wu, C. Li, and Q. Du, "Security threat analysis and corresponding countermeasures for hts communication system," in *Journal of Physics: Conference Series*, vol. 2246, 2022. [Online]. Available: https://doi.org/10.1088/1742-6596/2246/1/012010

[25] M. S. B. Mahmoud, N. Larrieu, and A. Pirovano, "An aeronautical data link security overview," in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, 2009, pp. 4.A.41–4.A.414. [Online]. Available: https://doi.org/10.1109/DASC.2009.5347501

[26] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *International Journal of Information Security*, vol. 20, pp. 287–311, 2021. [Online]. Available: https://doi.org/10.1007/s10207-020-00503-w

[27] T. Matus. (2021) Starlink vs. standard broadband: How do they compare & which is better? [Accessed March 30, 2023]. [Online]. Available: https://history-computer.com/starlink-vs-standard-broadband-how-do-they-compare-which-is-better/

[28] Microsoft Corporation. (2023) Microsoft threat modeling tool threats. [Accessed March 15, 2023]. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[29] MITRE Corporation. (2023) Threat assessment and remediation analysis (tara). [Accessed Feb. 3, 2023]. [Online]. Available: https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara

[30] National Institute of Standards and Technology. (2023) Nist risk management framework. [Online]. Available: https://csrc.nist.gov/projects/risk-management/about-rmf

[31] N.-T. Nguyen and C.-C. Chang, "A biometric-based authenticated key agreement protocol for user-to-user communications in mobile satellite networks," *Wireless Personal Communications*, vol. 107, pp. 1727 – 1758, 2019. [Online]. Available: https://doi.org/10.1007/s11277-019-06354-6

[32] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband," in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 277–284. [Online]. Available: https://doi.org/10.1145/3317549.3323418

[33] J. K. Pedersen, M. Bochman, and W. Meng, "Security analysis in satellite communication based on geostationary orbit," in *2022 19th Annual International Conference on Privacy, Security and Trust, PST 2022*, 2022. [Online]. Available: https://doi.org/10.1109/PST55820.2022.9851962

[34] Reverse Mode. (2022) Satcom terminals under attack in europe. [Accessed March 31, 2023]. [Online]. Available: https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html

[35] J. M. Rodriguez Bejarano, A. Yun, and B. De La Cuesta, "Security in ip satellite networks: Comsec and transec integration aspects," in *2012 6th Advanced Satellite Multimedia Systems Conference, ASMS 2012 and 12th Signal Processing for Space Communications Workshop, SPSC 2012*, 2012, pp. 281–288. [Online]. Available: https://doi.org/10.1109/ASMS-SPSC.2012.6333089

[36] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 50–61, 2005. [Online]. Available: https://doi.org/10.1109/MWC.2005.1561945

[37] SAAB. (2020) Signals intelligence - know your surroundings. [Accessed March 28, 2023]. [Online]. Available: https://www.saab.com/newsroom/stories/2020/october/know-your-surroundings

[38] A. D. Santangelo, G. Falco, and A. Viswanathan, "The linkstar cybersecurity "sandbox", a platform to test small satellite vulnerabilities within the community – updates and lessons learned," in *AIAA Science and Technology Forum and Exposition, AIAA SciTech Forum 2022*, 2022. [Online]. Available: https://www.researchgate.net/publication/357564523_The_LinkStar_Cybersecurity_Sandbox_a_platform_to_test_small_satellite_vulnerabilities_within_the_Community_-_Updates_and_Lessons_Learned

[39] J. D. Scanlan, J. M. Styles, D. Lyneham, and M. H. Lützhöft, "New internet satellite constellations to increase cyber risk in ill-prepared industries," in *Proceedings of the International Astronautical Congress, IAC*, vol. 2019-October, 2019. [Online]. Available: https://www.researchgate.net/publication/337499407_New_Internet_Satellite_Constellations_to_Increase_Cyber_Risk_in_Ill-Prepared_Industries

[40] K. Schilling and A. Dmitrienko, "Increasing security in satellite networks," in *Proceedings of the International Astronautical Congress, IAC*, vol. D5, 2021. [Online]. Available: https://www.researchgate.net/publication/357606031_Increasing_Security_in_Satellite_Networks

[41] Stratign. (2023) Direction finding system. [Accessed April 28, 2023]. [Online]. Available: https://www.stratign.com/direction-finding-system/

[42] K. Thangavel, J. J. Plotnek, A. Gardi, and R. Sabatini, "Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity," in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 2022-September, 2022. [Online]. Available: https://doi.org/10.1109/DASC55683.2022.9925759

[43] The Forum of Incident Response and Security Teams (FIRST). (2019) Common vulnerability scoring system version 3.1: Specification document. [Accessed March 15, 2023]. [Online]. Available: https://www.first.org/cvss/specification-document

[44] Time. (2021) Iran used protests over elon musk's satellite internet service to shut down the internet. what you need to know. [Accessed March 31, 2023]. [Online]. Available: https://time.com/6249365/iran-elon-musk-starlink-protests/

[45] U.S. Department of State. (2019) China's great firewall descends on hong kong internet users. [Accessed Jan. 16, 2023]. [Online]. Available: https://www.state.gov/joint-statement-on-internet-shutdowns-in-iran/

[46] ——. (2021) Joint statement on internet shutdowns in iran. [Accessed March 31, 2023]. [Online]. Available: https://www.state.gov/joint-statement-on-internet-shutdowns-in-iran/

[47] Versprite. (2020) What is pasta threat modeling? [Accessed March 15, 2023]. [Online]. Available: https://versprite.com/blog/what-is-pasta-threat-modeling/

[48] H. Wang, Q. Wang, W. Sun, N. Zhao, H. . Dai, and L. Xu, "Aerial assistant: Safeguarding ground-to-satellite communication networks," in *2022 IEEE Global Communications Conference, GLOBECOM 2022 - Proceedings*, 2022, pp. 964–969. [Online]. Available: https://doi.org/10.1109/GLOBECOM48099.2022.10000669

[49] L. Wouters. (2022) Glitched on earth by humans: A black-box security evaluation of the spacex starlink user terminal. [Accessed April 8, 2023]. [Online]. Available: https://www.youtube.com/watch?v=NXqLMmGwJm0

[50] X. Wu, Y. Du, T. Fan, J. Guo, J. Ren, R. Wu, and T. Zheng, "Threat analysis for space information network based on network security attributes: a review," *Complex and Intelligent Systems*, 2022. [Online]. Available: https://doi.org/10.1007/s40747-022-00899-z

[51] P. Yan, F. Chu, L. Jia, and N. Qi, "A cross-layer anti-jamming method in satellite internet," *IET Communications*, vol. 17, no. 1, pp. 121–133, 2023. [Online]. Available: https://doi.org/10.1049/cmu2.12516

[52] M. Zhuo, L. Liu, S. Zhou, and Z. Tian, "Survey on security issues of routing and anomaly detection for space information networks," *Scientific Reports*, vol. 11, no. 1, 2021. [Online]. Available: https://doi.org/10.1038/s41598-021-01638-z

Appendix A

Interview Questions

Below are the questions which were created for the interviews.

- **Satellite users**

  1. Can you walk us through the process of deploying the satellite internet system in high-risk zones, and what security measures are taken during the installation process?
     (a) Are there many units of satellite internet systems distributed so many people have their own unit, or are there more like hubs where people need to go in order to get an internet connection?
     (b) Are there any logistical aspects to the deployment of the satellite signal receiver? (Placement of the satellite dish X distance from the modem, camouflaging the dish, etc)
     (c) How does the satellite internet system accommodate different types of devices, such as smartphones, laptops, etc?
     (d) What is the main use of the satellite internet system?
     (e) What are the main ways of communication used? (email, chat services, Voice-calls or video calls for example)
  2. When you received these systems,
     (a) Were you instructed on any potential risks with using the satellite internet system, for example:
        – Jamming
        – Eavesdropping
        – Spoofing
        – Tracking
        – Other risks (Please provide a description of the risks)
     (b) Were there any directions, guidelines, or best practices (for example: Not using the system during certain hours) that were recommended to you for secure usage of the satellite internet systems?
     (c) Were there any security measures (for example VPNs or encrypted emails) that were recommended to you for secure usage of the satellite internet system?
     (d) If the answer to any of the three previous questions was yes, what was the source of information (for example SpaceX, Military, or the Government) for each?

3. Have you experienced any attacks against the system, be they physical or software related?
   (a) If so, can you describe what form of attack it was?
   (b) If any, what were the consequences of the attack?
   (c) Is there any contingency plan for if the network is compromised or becomes unavailable? If yes, can you discuss it
4. What steps are taken to protect the satellite internet system from physical damage or theft?
   (a) Are there any contingency measures that you have in place in case the system is physically compromised, for example: erase data or a killswitch?
5. Can you discuss any feedback or concerns you have, or have received from other users of the satellite internet system?
   (a) Has any of the feedback been addressed?
6. Finally, is there something else related to the topic of our questions that we did not ask about but that you think would contribute to our study?

- **Satellite developers**

1. What are some vulnerabilities and/or shortcomings that you are aware of that exist in satellite network systems today?
   (a) Where in the network structure (User station, Ground gateway, Radio Frequency connections, or the satellite itself) do these vulnerabilities/shortcomings exist?
   (b) Are there any solutions to these vulnerabilities/shortcomings that you know have been implemented into the systems recently or are coming in the near future?
   (c) Are there any of these vulnerabilities/shortcomings that you do not see a solution to, that will continue to be an issue in the future?
2. From an outside perspective there seems to be a lot of advancements being made in the area of satellite communications, for instance, satellite internet and its availability to everyday people. In terms of security, what recent advancements do you think are the most impactful?
3. In your opinion, what area of satellite communication security is currently lacking progress?
4. Have you performed a risk analysis or other forms of assessment of the security of satellite internet? If yes, what was the result?
5. What are some recommendations and/or information that you believe is important to know for someone utilizing satellite internet technology?
   (a) Are there any measures that you know of that a user of satellite internet technology could utilize in order to make sure their connection is private?

6. Finally, is there something else related to the topic of our questions that we did not ask about but that you think would contribute to our study?

- **Risk managers**

1. In a warzone, potential threat actors could have access to more resources. We saw this in February of 2022 when Viasat modems were rendered inoperable in Ukraine by malware.
   (a) If a client were to travel to a part of a warzone, would you consider satellite connection a viable option for internet access?
   (b) What are some risks you would consider before utilizing satellite internet in this type of area?
   (c) Do you believe it is possible to distinguish between a civilian and a military target in these areas?
2. If you were to use satellite internet in a warzone, would it be a military-grade connection or a connection that would also be available to civilians?
3. When evaluating the risks in a warzone,
   (a) What type of different threat actors do you see?
   (b) What are some assumptions you would make about the capabilities of each threat actor?
4. What are your opinions on the security of satellite communication as a means to connect to the internet?
   (a) Would you treat the connection as secure "as-is" or would you employ other security measures?
   (b) If other security measures would be used, what type of security measures would that be?
5. Have you performed a risk analysis or other forms of assessment of the security of satellite internet? If yes, what was the result?
6. Finally, is there something else related to the topic of our questions that we did not ask about but that you think would contribute to our study?

Appendix B

Interviews

In this appendix, the anonymized transcriptions of the interviews performed in this work are presented.

B.1 Private security companies

The following interviews were conducted with participants who work at companies dealing with private security.

B.1.1 Transcript of interview 1

Interviewer - What is your role in your company?

Interviewee - I'm the head of international services and a strategic adviser with *Security company.*

Interviewer - And what is your previous experience with satellite internet?

Interviewee - I've worked as an officer in the Country's military and with various non-government organizations deploying to different conflict zones and national disaster-affected areas, where we've had to rely on satellite communications.

Interviewer - So, to our questions.
- From our perspective, in a Warzone, a potential threat actor could have access to more resources. We saw this in February of 2022 when Viasat modems were rendered inoperable in Ukraine by malware. If a client were to travel to a part of a warzone, would you consider satellite connection a viable option for Internet access, seen from a security perspective?

Interviewee - Well, I guess it always comes back to what risk we're trying to mitigate. If the risk we're trying to mitigate is being identified by the government actors, then the answer would be no. But if the risk you're trying to mitigate is the client losing communications and needing to be able to organize evacuations or get intelligence on whether it's safe to move, then the answer would be yes, we would advise them to take it with them as backup communication.

Interviewer - What are some risks you would consider before selecting satellite internet as a means of communication in this type of area? And I guess you answered that in the previous questions, but are there any other risks that you would consider?

Interviewee - We would look and see if there's any relevant legislation around the use of satellite communications. We'll look at normal practices and modus operandi within the area, and if anyone is using satellite communications. For example, a group of Europeans who would turn up with fancy communications is likely to draw attention to them and increase their risk profile. So, we're certainly looking at those.

Interviewer - Do you believe it's possible to distinguish between a civilian and a military target in these areas?

Interviewee - No.

Interviewer - Are you aware if it is possible to remotely locate someone who is utilizing a satellite connection?

Interviewee - Yes, government actors can certainly do that.

Interviewer - If you were to use satellite internet in a war zone, would you use the equipment available to the military or would it be a connection that would also be available to civilians? For example, something like Starlink?

Interviewee - We would only use civilian equipment. Since we are a civilian organization, we don't have access to any military equipment.

Interviewer - When evaluating risks in a war zone, what type of different threat actors do you see? You mentioned before that there are government actors, but are there any other types of threat actors you'd consider? For example, some professional groups in the area?

Interviewee - So, there are the parties of the conflict. They could be state or non-state actors that are shooting each other. There could also be criminal actors that are profiting from the environment, which could mean a risk to personnel using satellite communications. Additionally, there could be opportunistic civilians who might see an opportunity for enrichment, or they might see the conflict as a waste of funding that could be otherwise spent feeding them, or the general civilian population.

Interviewer - Do you make any assumptions about the capabilities of these threat actors? Do you research them beforehand, or do you have a set of assumptions you make?

Interviewee - We'll always do research to identify who the key actors are, their modus operandi, and how they have reacted toward the people that we're representing. Whether it's journalists, bankers, Italian workers, French people, Israelis, or Americans, they are all going to have different risk profiles, fat people, skinny people, they're all going in with different risks and vulnerabilities. So, we need to understand how the interplay is going to occur between the different actors in the destination.

Interviewer - What are your opinions on the security of satellite communication as a means to get internet access? And would you treat the connection as secure as is, or would you employ other additional security measures in these connections?

Interviewee - No, I would treat satellite communications as secure as any other type of communication, it can be intercepted, listened to, and traced. But generally, for our clients, the advice is that anything they're doing should be transparent, and if it's not then they really need to consider what they're doing when communicating that, whilst still being in the country.
- An example of that could be journalists in China investigating human rights abuses. Maybe they'd be best off communicating that when they leave China or should submit their stories after they've left the country. So yeah, we wouldn't employ satellite internet because again, if they need to employ encryption or additional security measures, then they run the risk of drawing additional attention to themselves.

Interviewer - Have you performed a risk analysis or other forms of assessment of the security of satellite internet?

Interviewee - No, because we assume it's not secure.

Interviewer - So, is it just the assumption that it's not secure, and no analysis needs to be done? And you do treat it like a regular Internet connection, and just assume that it is open and there's nothing special about it?

Interviewee - That's right.

Interviewer - Is there anything that relates to the topic of our questions that we did not ask about? So is there something in your experience or that you've learned about using satellite communications, which we did not ask about now, but you feel would be helpful to us in our study?

Interviewee - I think the potential thing is the utility of satellite communications. And what we have seen is that, for comparison, in 2005 we were utilizing satellites as a necessary means of communication every single day. Whereas in the last eight years, I think in 2014 we're utilizing it quite a bit in Central Asia, but since then there's very little need to be using satellite communication.
- Now I know in Ukraine there has been a benefit from using Starlink, certainly for military actors, but you know that's a rare occasion. I was in Ukraine recently and had no problems with communications with regular mobile phones. So, I think the need for satellite communications is decreasing, at least from our experience or my experience. It's less and less necessary. As it used to be, you'd have to travel with a big bag, if you'd have to travel with an Inmarsat or Thuraya. Yeah, it is very rare that you need these things.

B.1.2 Transcript of interview 2

As this interview was performed in Swedish the English translation is provided below followed by the original. Important to note is that three interviewees from the same company were present during this interview.

English translation:

Interviewer - What is your role in the company?

Interviewee - CEO and Founder, Head of IT, Operations manager

Interviewer - Do you have any experience with satellite internet?

Interviewee - Yes, it is not used very often, primarily as a backup. Very rarely are you in places where there is no other access. Even the most worn-down places often have some other way of establishing a connection.

Interviewer - In a warzone, potential threat actors could have access to more resources. We saw this in February of 2022 when Viasat modems were rendered inoperable in Ukraine by malware.
- If a client were to travel to a part of a warzone, would you consider satellite connection a viable option for internet access?

Interviewee - Absolutely but primarily as backup. In the case of Viasat, it was specifically a supply-chain problem and as such it did not matter that it was satellite communication involved.

Interviewer - What are some risks you would consider before utilizing satellite internet in this type of area?

Interviewee - It depends on what you are doing there, what is the purpose? For purely civilian purposes it is not necessary.
- From satellite internet you can get a lot of information about who is talking to whom.

Interviewer - Do you believe it is possible to distinguish between a civilian and a military target in these areas?

Interviewee - Absolutely, on a tactical level they can be dangerous because you can make the assumption that an emitter is military when it shouldn't be there.

Interviewer - If you were to use satellite internet in a warzone, would it be a military-grade connection or a connection that would also be available to civilians?

Interviewee - No, we would never use military systems for several reasons. For example, one does not want to be misinterpreted as being associated with the military.

Interviewer - When evaluating the risks in a warzone, what type of different threat actors do you see?

Interviewee - From host nations or other nations in the area, but also extremist organizations.
- You also have to make an evaluation of which actors are in the area, both potential threats but also your own "partners", even if you know who they are this does not mean that you can trust them.
- When it comes to satellites, you also get some transferred risk. You can see directly in a crisis situation what satellite technology is being used and you are visible to outside parties.

Interviewer - What are some assumptions you would make about the capabilities of each threat actor?

Interviewee - It depends on who you are and what you do there, and who would be the primary threat actor in that case?
- If you are there for humanitarian reasons it could be, for example, the ruling power in the country.
- It is on a case-by-case basis, for example in Colombia where local actors got access to techniques, for example, to intercept phones, that really only nation-states should have access to.

Interviewer - What are your opinions on the security of satellite communication as a means to connect to the internet?

Interviewee - It can be assumed that the cryptography can be cracked and the data can be read. Some powerful states can be assumed to have the capability to crack cryptography if they wanted to. It also depends on the device being used as well as the implementation of the cryptography it uses.

Interviewer - Would you treat the connection as secure "as-is" or would you employ other security measures?

Interviewee - The connection per se is not secure. In order to secure the network, in that case, you have to set up your own tunnel, and your own encryption.
- Communication "Lights up" enormously when in use.
- The satellite is connected to a system, which means that the manufacturer can always see where you are.
- If the system is running, it can be tracked.
- It is also very difficult to travel into countries where these systems would be used, for example, for humanitarian purposes, as the country's ruling power might not consider it permissible to bring them in.
- If satellite communication is used in such an area the system needs to be set up somewhere to begin with. You should also be quick when using the connection so the risk of revealing your position is reduced, you should not stay in the same place for too long, and you should not use the connection in your hotel room. It's not easy.

Interviewer - Have you performed a risk analysis or other forms of assessment of the security of satellite internet? If yes, what was the result?

Interviewee - It is possible that we have done it, but we have no idea what specific system it would have been done for, but we have reasoning around different systems.

Interviewer - If you were to do risk analysis today, which method would be used?

Interviewee - We would use a common method of risk analysis. We should probably start looking at probability and consequences, i.e. what is the probability that the risk will occur and what consequences will result from it. MSB (The Swedish Civil Contingencies Agency) is usually a common reference point for such analysis.

Interviewer - Finally, is there something else related to the topic of our questions that we did not ask about but you think would contribute to our study?

Interviewee - Generally speaking, it is very difficult to make an assessment of what you are going to do if you do not have that knowledge beforehand. It requires people who are experienced in gathering information in order to reach the right conclusions.
- In general, satellite systems can be assumed to be very visible, since they, as mentioned earlier, "light up" when in use and can be seen by other parties who monitor such activity.
- From an operational point of view, you can do simple things like coding your language to protect communication when making future plans.
- Even if you get a new device, for example, a phone which when new cannot be directly associated with you, you may call a number you have called before which can allow the new device to be associated with you because of the recipient of the call, and that way you can still be seen.

Swedish original

Intervjuare - Vilka roller har ni i företaget?

Intervjuperson - Vd och grundare, IT-chef drift och support, Operativa delarna.

Intervjuare - Har ni någon tidigare erfarenhet av satellit internet?

Intervjuperson - Ja, det används inte särskilt ofta, mer som backup. Väldigt sällan man är på ställen där det saknas annan access. Även de mest nedgångna platser har ofta något sätt att koppla upp sig i alla fall.

Intervjuare - I en krigszon kan potentiella hot-aktörer ha tillgång till mer resurser. Vi såg detta i februari 2022 när Viasat-modemen blev obrukbara i Ukraina på grund av ett malware. Om en klient skulle resa till en del av en krigszon, skulle du överväga satellitanslutning som ett lämpligt alternativ för internetåtkomst?

Intervjuperson - Absolut, framförallt som backup. I Viasats fall var de specifikt ett supply-chain problem så hade inte spelat roll att de var satellit.

Intervjuare - Vilka är några risker du skulle överväga innan du använder satellitbaserat internet på denna typ av plats?

Intervjuperson - Det beror på vad ska man göra där, vad är syftet? I rent civila syften så är de inte nödvändigt.
- Från satellitinternet kan man få ut väldigt mycket information från vem som snackar med vem.

Intervjuare - Tror du att det är möjligt att skilja mellan en civil och en militär måltavla på dessa områden?

Intervjuperson - Absolut, på en taktisk nivå så kan det vara farligt eftersom man kan göra antagandet att en emitter är militär då den inte ska vara där.

Intervjuare - Om du skulle använda satellit-internet i en krigszon, skulle det vara en anslutning av militär klass, eller en anslutning som också skulle vara tillgänglig för civila?

Intervjuperson - Nej, vi skulle aldrig använda militära system av flera anledningar. Man vill exempelvis inte bli misstolkad som militärt associerad.

Intervjuare - När du utvärderar riskerna i en krigszon, vilka typer av olika hot-aktörer ser du?

Intervjuperson - Alltifrån värdnationer eller andra nationer i området, men även extremistorganisationer.
- Man får även göra en utvärdering på vilka aktörer som finns i området, både potentiella hot men även ens egna "partners". Även om man vet vi vilka de är, betyder inte att man kan lita på dem.
- När det kommer till satelliter får man också en viss överförd risk. Man kan se direkt i en krissituation vilken satellitteknik som används samt att man är synlig för utomstående parter.

Intervjuare - Vilka antaganden skulle du göra om förmågorna hos varje hot-aktör?

Intervjuperson - Det beror på vem man är och vad man gör där, samt vem som i så fall skulle vara den primära hot-aktören.
- Om man är där av humanitära orsaker så kan det till exempel vara den styrande makten i landet.
- Är på Case-by-Case basis, till exempel i Colombia där lokala aktörer fått tillgång till tekniker, exempelvis att avlyssna telefoner eller tekniker som egentligen bara stater ska ha tillgång till.

Intervjuare - Vad är era åsikter, sett ur ett säkerhetsperspektiv, om satellitbaserad anslutning som ett sätt att få åtkomst till internet?

Intervjuperson - Man får anta att krypton kan knäckas och data kan läsas. Vissa kraftfulla stater kan man anta har kapabilitet att knäcka krypton om de bara skulle vilja. Det beror också på enheten som används samt implementationen av kryptot som den använder.

Intervjuare - Skulle du behandla satellit-anslutningen som säker "som den är" eller skulle du använda andra säkerhetsåtgärder för att säkra nätverket?

Intervjuperson - Anslutningen per-se är inte säker. För att säkra nätverket får man i så fall sätta upp sin egen tunnel, och egen kryptering.
- Kommunikationen "Lyser upp" enormt mycket när det används.
- Satelliten är uppkopplad i ett system vilket gör att tillverkaren alltid kan se vart du finns.
- Är systemet igång så går det att spåra.
- Det är även mycket svårt att resa in i länder där dessa system skulle användas för till exempel humanitära ändamål då landets styrande makt kanske inte skulle anse det som tillåtet att ta med sig in.
- Om satellitkommunikation används i ett sådant område, behöver systemet

till att börja med sättas upp någonstans. De bör även gå fort när man väl använder anslutningen så risken minskar att man avslöjar sin position, man bör inte stanna på samma ställe för länge, förslagsvis inte koppla upp sig på sitt hotellrum. Det är inte helt lätt.

Intervjuare - Har du utfört en riskanalys eller andra former av utvärderingar av säkerheten i satellitbaserat internetsystem? Om ja, vad var resultatet?

Intervjuperson - Det är möjligt att vi har gjort det, men vi har ingen aning om vilket specifikt system det skulle blivit gjort för, men har resonemang runt olika system.

Intervjuare - Om ni skulle göra riskanalys idag, vilken metod skulle användas?

Intervjuperson - Vi skulle använda en vanlig metod för riskanalys. Vi skulle väl börja titta på sannolikhet och konsekvenser, alltså vad är sannolikheten att risken inträffar och vilka konsekvenser kommer av det. MSB (Myndigheten för Samhällsskydd och Beredskap) brukar vara en vanlig referenspunkt för sådana analyser.

Intervjuare - Slutligen, finns det något annat som är relaterat till ämnet som vi inte frågade om , men som du tror är information som skulle bidra till vår studie?

Intervjuperson - Rent generellt är det väldigt svårt att göra en bedömning av det ni ska göra om man inte har den kunskapen sen innan. Det kräver folk som är erfarna av informationsinhämtning för att man ska kunna komma fram till rätt slutsatser.
- Rent generellt kan satellit-systemen tolkas som väldigt synliga, då de som nämnt tidigare “lyser upp” vid användning och kan ses av andra parter som övervakar sådan aktivitet.
- Ur ett operativt synsätt, så kan man göra enkla saker som att koda sitt språk för att få en mer skyddad kommunikation.
- Även om du skaffar en ny enhet, till exempel en telefon som i nyskick inte direkt kan associeras till dig, så kanske du ringer ett nummer du ringt innan vilket gör att den nya enheten kan associeras till dig på grund av mottagaren av samtalet, och på så sätt syns man ändå.

B.2 Satellite developers

The following interview was conducted with a participant working in a company that deals with, among others, engineering and security regarding satellites.

B.2.1 Transcript of interview 3

Interviewer - What is your role in your company?

Interviewee - I'm the chief defense, security, and technology strategist. So, I work directly with the CEO in establishing the company direction in terms of the markets, the technologies, the sectors that the company is involved with, as well as the company structure and the business direction that we wanna take, so I am basically helping the CEO run the company in large part.

Interviewer - In terms of satellite or satellite internet, what is your experience in that field?

Interviewee - Well, I used to be a military officer and a telecommunications officer for the *country's* military. When I left the military, I was responsible for all the strategic networks, signals intelligence, electronic warfare, and cyber operations for the Armed Forces, and then I spent three years at the *Country* Cyber-Command doing their strategic policy plans and force development. So throughout all this, when I was running the *Country's* forces network I was responsible for SATCOM networks among everything else. Many years ago, this would have been in the early to mid-90s, I set up our satellite communications unit, the formation that provided strategic communications for the *Country's* forces, and just part of my education, I did some Masters level courses on satellite communications, but that's many, many years ago. So I've got some theoretical background as well as management experience and project experience.

Interviewer - In your experience, what are some vulnerabilities or shortcomings of satellite network systems today? Or if you have some past shortcomings of the systems you are aware of?

Interviewee - Well, I guess from my perspective it was somewhat of an evolution in the vulnerabilities because historically the satellite communications industry has been a very conservative industry from an engineering, program management, and development standpoint. They would use more proprietary standards. So some of the legacy systems, the geosynchronous systems, are traditional infrastructure and they really weren't designed with security in mind. They weren't really seen to be a threat. And I think that was kind of largely in the satellite communications community unless it was the government or military communities. In the commercial environment, there really wasn't a culture of security per se. They really focused on functionality and when you take a look at the economic pressure to maximize the bandwidth. I mean there are lots of very interesting things that have been done from a coding perspective in terms of getting information efficiency through the network environment, but security has been something that hasn't been really taken seriously. It's kind of fallen to the back seat.

- But now I would say when we look at the evolution of satellite capabilities, even the traditional systems, the user stations, the ground gateways, the radio frequency (RF) connections, these have largely been discrete proprietary protocols in large part isolated from the Internet. Now what we're seeing is that the connectivity in a number of these systems is increasingly relying on Internet infrastructure. The stuff we're doing with the European Space Agency when you take a look at remote connectivity and also the service provisioning side, it's dramatically changed over the last 20 years. You're operating missions through the Internet, your supply arrangements are exercised through the Internet. You're using much more commercial off-the-shelf (COTS) products which have their own concerns from a supply chain perspective as well. So that provides a significant piece. Then as well the RF connections, again with the evolution of the software-defined radio technology, onboard the bird, the

ground stations, the availability of these protocols. I mean probably in your research you've come to see that there are all sorts of commercially available products that can be used to connect to many of the satellites.
- My hobby is amateur radio, so I've been building satellite links, antennas and using radios, communicating through some of the amateur radio birds, and have been involved in some of the small initial CubeSats 20-30 years ago and it's remarkably easy to be able to access these things. Probably in part of your research, you can see that there are all sorts of activities and capabilities that allow you to do that. So I'd say when we look at the evolution of satellite systems and their increasing infrastructure interconnection with terrestrial infrastructure, what we're seeing is that in a lot of the remote parts of the world, especially for example, Africa where satellite infrastructure is now usurping the traditional terrestrial role, that poses some significant challenges. In countries like China are looking to take advantage of that environment and assert themselves. Culturally since the environment developing satellite networks hasn't been there, you see a lot of vulnerabilities and threats developing in these environments.

Interviewer - You mentioned our research there and what we've seen is a researcher was able to eavesdrop on satellite communications and they saw that a lot of the communication was sent as clear text. If a researcher could do this with only $300.00 equipment, what capabilities could an adversary with access to more resources possess?

Interviewee - Absolutely. I mean we saw that a lot of the hobbyists use C-band and Ku-band to access the television signal. The encryption that was provided on those links is easy enough to break. If you're looking at government links, state actors have very advanced cryptographic capabilities. I mean these are things that they would devote specific effort to and can easily break.

Interviewer - Working in the field do you think there are any solutions to these vulnerabilities or shortcomings that are on the way or do you think these problems will still be there in the future?

Interviewee - There's certainly an evolution that's taking place. So for example we do a lot of work with the European Space Agency (ESA) and The European Union Agency for the Space Program (EUSPA) which historically has been involved in the Galileo program, and there's always been a pretty robust security construct programmatically around that, but the European Space Agency largely had a very altruistic, benevolent approach in the culture surrounding it. There's a significant awakening of the need for security because they're providing capabilities, particularly in the areas of Earth observation. When we take a look at the reliance on critical infrastructure that supports government legitimacy and societal resiliency, we see its dependency, its linkage to critical infrastructure, and the critical infrastructure dependency on both space capabilities, be it communications, position, navigation, timing or earth observation in the programs that ESA develops, you're seeing them become much more seized with the importance of doing this, and a lot of these programs support European

interests.
- So from a policy perspective they've put a significant amount of effort into developing a policy construct. They're developing a security operations center to try to coalesce the oversight and management of the different missions from a security perspective, and then they're also developing a center of cyber security, Center of Excellence, and we're involved with supporting them in these initiatives and helping them develop that. So we're developing the SOC for them and we're also helping them develop the cyber security center of excellence. There's been a number of projects that we've been involved in in terms of supporting them, in terms of developing the doctrinal framework for cyber security. So for example taking the MITRE attack framework, which historically has been really focused on terrestrial infrastructure, adapting it to the space environment, and then helping from an architectural perspective to look at evolving how that is applied. That introduces some new elements of discussion in and around cyber security as it applies to the satellite area. So things like zero trust architectures and the quantum key distribution pieces are able to make the links more robust.

Interviewer - We've seen some research on quantum key distribution so it's very interesting that they try to apply it. We hadn't heard about applying MITRE to satellite security, but it makes sense.

Interviewee - That's an approach we've taken because one has to remember that satellite infrastructure is a kind of extension of terrestrial infrastructure. So when you're looking at developing doctrinal concepts and also technical constructs that have to be able to respond in these environments while also using analogous and well-understood frameworks there will be appointed departures that are important for coherency.

Interviewer - Are there attributes of satellite communication systems that will stay vulnerable?

Interviewee - There are a few elements. I would say the radio frequency spectrum pieces, that's always a challenging element because you know jamming and spoofing, jamming in particular. I mean that's a radar equation function. That's a lot of physics-type of things. So I mean you're always gonna be vulnerable to that depending on where you can position your transmitters, the antennas, notwithstanding the fact that you can apply smart technologies in terms of having agile antennas, smart antennas on satellite systems, and whatnot. I mean programmatically that takes quite a bit of time to do. You can identify what the risks are, but putting a satellite into space, a significant one, it's an expensive piece. So when you're looking at the increasing commercial reliance on LEOs and CubeSats, which are just limited in and of themselves, I would say there's a programmatic challenge. There's only so much physics that you can cram into a small device like that, so I'm not sure if that's solely laws of physics, but it's kind of at the intersection of laws of physics and financial considerations.
- So there's that piece, and then you start to get into quantum capabilities

again. These are challenges and those are kind of tied to how quickly practical quantum cryptography can be implemented because already there's data that's being captured and stored for ultimate decryption in time. So the horse may already have left the barn on that one. So there's that if you're talking in terms of what can't be resolved in short order. Again being able to practically implement that across international infrastructures is a challenge. Given all the challenges of having the right technologies, the right supply chains, the right programs, and ensuring that you have interoperable standards. So, this is all new stuff and we're working on a quantum key distribution program right now and these are kind of practical issues that are starting to come to the fore. It's one thing to do a demonstration, it's another thing to do that in a repeatable way that can be industrialized.
- So, I'd say when you're looking at what can't change, I mean anything could be changed, but it just gonna be a matter of time and what information in that intervening time has been exposed and potentially lost.

Interviewer - What recent advancements in terms of security have you seen and what impact do you believe these advancements will have?

Interviewee - Yeah, I mean it's a broad general principle. It's like most things awareness in professional development is kind of at the forefront, that's what I think is the seed of this, having training and awareness. So you know for example a lot of the work we do with the ESA and increasingly with the industry is training. Not only the engineers but also senior executives that become seeds with the issue, program managers, and operators, so they understand it's changing the culture of the business. People who historically just haven't looked at security. So that's one element that then triggers many other things I would say.
- With government agencies, what we're seeing is, and you're seeing it at a very senior level within Europe, that they're taking programs like GOVSATCOM, Galileo, and Copernicus and putting these programs under a federal authority structure, to identify critical communications systems that will have the oversight, but it takes advantage of security organizations. You know the disciplines and understanding of security from these organizations.
- Then commercial satellites upon which some simple applications may reside, or some government services may end up taking a lesser responsibility. So there's a risk mitigation effort going on in terms of triaging and saying this demographic of satellite capabilities may be commercial. LEO like Starlink will be useful but they'll have limited utility. And so you're starting to see a triaging of what infrastructure is tied to different types of satellite carriers.
- Also the efforts put in place in terms of securing the supply chain, bringing critical chip technologies closer. For example, in the US in North America, and in Europe to secure that piece of technology, you see things like the evolution of zero-trust architectures. Now as we start to see the integration of civil and government capabilities and taking these different approaches to securing satellite systems and their complexity I think those are kind of the methodologies that you're starting to see take place.

Interviewer - Have you performed any risk analysis or other forms of assessment of the

security of satellite internet?

Interviewee - Oh yeah.

Interviewer - Can you share some of the results of these? If it's too much, maybe a general idea of the results?

Interviewee - Yeah. So that's one of the main services that our company provides. So we've done quite a number of those, like for example for the ESA networks and a number of commercial networks. In large part, if I had to characterize a lot of the results of the risk analysis, it really comes down in many cases to poor user awareness of security and that goes across the different demographics, senior leadership, operators, engineers, and managers understanding and appreciating the risks. So that's one of the key areas.
- The radio frequency links most certainly are a significant risk and we've seen that even recently in the Ukraine war that those have been negated. The Viasat hack, a network that supposedly provides critical support to military capability and it was almost trivial to be knocked off.
- There's an increasing awareness of the nature of the threats, be it kinetic, physical, cyber, or electronic warfare. In all those different categories there are either state actors, criminals, or private actors that will assert efforts at one level or another to achieve whatever aim. It's not just data but there's a lot of criminal interests.
- The traditional Consultative Committee for Space Data Systems (CCSDS) protocols that have been used in the space industry again haven't had security built in. So that's a significant vulnerability. You can point to virtually any element of the field and see that it's an industry that's not unlike the initial stages of the Internet. The internet when it was developed, ARPANET, was built based on a network of known trusted users. But right now the network environment has exploded. Most of the users that communicate are not known, they're untrusted and the industry has to evolve to face that. So we're probably a step behind the traditional terrestrial cyber security environment, but with the increasing interconnection of space infrastructure with the terrestrial infrastructure, it's now got to be treated with the same veracity.

Interviewer - Are there any recommendations or information that you believe would be important for someone utilizing satellite internet technology, anything important that they should keep in mind when doing so?

Interviewee - A lot of it depends on the demographic who is using the system. So if it's a government entity providing very critical capabilities, you need to really understand the use case and understand the technology and potential risks. When I say potential risks I mean understanding who is likely to be interested in penetrating your network and disrupting it or destroying it. So really understanding what are the threats to the network and the vulnerabilities of the potential technology. Really doing a comprehensive threat risk analysis and doing that at the start while you're dividing the network development so that you could integrate the development of cyber security as an active element in

the design of the network.
- What we found is that in many cases the network is blind and then security is just tacked on as a nice to have at the end. If you do it that way, then it's not gonna be integrated effectively and you're gonna make shortcuts. So I would say that security has to be considered as a fundamental operational element, a key requirement that is characteristic of the network and integrating these types of methodologies in place and looking at the new emerging disruptive technologies.

Interviewer - Finally, is there something related to the topic of our questions that we did not ask about, but you think would contribute to our study? So is there something else you would like to add that we didn't ask about?

Interviewee - Well, I mean I think we've covered most of the issues, the topics.

Interviewer - Alright, thank you.

B.3 Satellite internet users

Below are the answers we received from users who had utilized satellite internet in a high-risk area. The questions were answered as a questionnaire and no interviews were conducted in this case. When a question did not receive an answer we instead have written "*No answer*".

Question - Are you in the military or civilian?

Answer - Civilian

Question - What experience do you have with satellite internet?

Answer - Home usage experience. Deployment, initial configuration.

Question - If you are a civilian and your experience with satellite internet is tied to the company you work at, what does your company do (In general) and what is your role in the company?

Answer - I deployed Starlink at home for home usage.

Question - Can you walk us through the process of deploying the satellite internet system in high-risk zones, and what security measures are taken during the installation process?

Answer - *No answer.*

Question - Are there many units of satellite internet systems distributed so many people have their own unit, or are there more like hubs where people need to go in order to get an internet connection?

Answer - *No answer.*

Question - Are there any logistical aspects to the deployment of the satellite signal receiver? (Placement of the satellite dish X distance from the modem, camouflaging the dish, etc)

Answer - Starlink antenna cable length is 32 meters (by default, but can be longer). The antenna looks north so there should not be anything between the antenna and the satellites.

Question - How does the satellite internet system accommodate different types of devices, such as smartphones, laptops, etc?

Answer - The model has built-in WIFI, so it is possible to buy an ethernet adapter.

Question - What is the main use of the satellite internet system?

Answer - Backup internet link.

Question - What are the main ways of communication used? (email, chat services, Voice calls or video calls for example)

Answer - Do not have any experience in communication with support.

Question - When you received these systems, Were you instructed on any potential risks with using the satellite internet system, for example:

- Jamming
- Eavesdropping
- Spoofing
- Tracking
- Other risks (Please provide a description of the risks)

Answer - No

Question - Were there any directions, guidelines, or best practices (for example: Not using the system during certain hours) that were recommended to you for secure usage of the satellite internet systems?

Answer - *No answer.*

Question - Were there any security measures (for example VPNs or encrypted emails) that were recommended to you for secure usage of the satellite internet system?

Answer - No

Question - If the answer to any of the three previous questions was yes, what was the source of information (for example SpaceX, Military, or the Government) for each?

Answer - No

Question - Have you experienced any attacks against the system, be they physical or software related?

Answer - No

Question - If so, can you describe what form of attack it was?

Answer - *No answer.*

Question - If any, what were the consequences of the attack?

Answer - *No answer.*

Question - Is there any contingency plan for if the network is compromised or becomes unavailable? If yes, can you discuss it

Answer - *No answer.*

Question - What steps are taken to protect the satellite internet system from physical damage or theft?

Answer - It is placed on my balcony. Only I have physical access to all components.

Question - Are there any contingency measures that you have in place in case the system is physically compromised, for example: erase data or a killswitch?

Answer - *No answer.*

Question - Can you discuss any feedback or concerns you have, or have received from other users of the satellite internet system?

Answer - *No answer.*

Question - Has any of the feedback been addressed?

Answer - *No answer.*

Question - Finally, is there something else related to the topic of our questions that we did not ask about but you think would contribute to our study?

Answer - *No answer.*

Appendix C

Practical guide

In this appendix, the final version of the practical guide is presented, beginning on the following page.

Satellite internet usage in high-risk areas

Information and safety guidelines

Andreas Kvant & Carl Johansson

Contents

Abbreviations

CIA Confidentiality, Integrity, Availability. 19, 23

GEO Geostationary Earth Orbit. 6, 7

ISP Internet Service Provider. 6, 8

LEO Low Earth Orbit. 6, 7

MEO Medium Earth Orbit. 6

NGEO Non-Geostationary Earth Orbit. 6

VPN Virtual Private Network. 22

VSAT Very Small Aperture Terminal. 3

Chapter 1

Introduction

Before we begin we would like to provide some information about the project on which this document is based. We will also give a description of the document's overall structure, as well as the intended use of this document.

1.1 About this project

This document is produced as a result of the Master's Thesis "Secure satellite internet usage in high-risk areas".

The authors are at the time of writing two students working on our master's thesis to graduate from the "Master of Science in computer security" program at Blekinge Institute of Technology in Karlskrona, Sweden. This project has been done in collaboration with Knowit Cybersecurity and law, and Civil Rights Defenders, who saw the use of satellite-based internet as a potential solution to achieve internet connectivity in high-risk areas when the terrestrial internet infrastructure fails due to damage, shutdown, or antagonist interference.

The purpose of our thesis was to review the research on the subject of satellite security while also gaining insight from experts in the field of satellite communication as well as experts in the field of security and risk assessment. Through these sources, we have attempted to find threats, vulnerabilities, and risks of using satellite internet in high-risk areas or satellite internet usage in general, as well as to find possible mitigations to these problems.

The results of our study have then been compiled into this document which is intended to provide information and guidelines for secure and safe usage of satellite internet communication. This practical guide as we have chosen to call it is aimed towards people and organizations who operate in high-risk areas that consider satellite internet as a potential means of communication but may not have the technical insight into the security and safety issues that accompany satellite internet usage.

1.2 Structure of the guide

This document is structured in the following way:

1. **Satellite internet fundamentals** - In this chapter, we will provide some information about the satellite internet infrastructure, functionality, and how it ties into traditional terrestrial internet communication.

2. **Common threats and risks** - This chapter will provide an overview of common threats, vulnerabilities, and risks associated with the use of satellite internet in high-risk areas but also in the general case of satellite internet usage.

3. **Risk assessment** - In this chapter, we will present the results of the risk assessment performed in the thesis. We will explain how threats and risks have been assessed as well as ranked in order of severity and impact and also the reasoning behind the rankings.

4. **Best practices** - In this chapter, we present and suggest some mitigations to the threats and risks that have been discussed in previous chapters, as well as best practices for the safe usage of satellite internet systems.

1.3 Scope and Disclaimer

Since this document is based on the more extensive project of a Master's thesis, it is also limited by the scope of that project. For this reason, some aspects of satellite internet security may not be included in this document.

This document is intended to provide general information about satellite internet and its safe usage in high-risk areas. The guide takes into consideration the different parts of satellite internet communication systems e.g. the Ground-station gateways, the user equipment, and the satellite itself. The user equipment the document concerns is Very Small Aperture Terminal (VSAT) whose intended use is internet access, it does not take into consideration satellite phones, positioning devices, or similar equipment. The practical guide does not provide specific details about individual satellite Internet systems or services.

Also since satellite internet systems are an extension of the terrestrial internet, although operating in different ways, many of the threats, risks, and vulnerabilities that accompany the usage of terrestrial internet will be inherited by the satellite internet infrastructure. For this reason, this document should also be considered as dealing with an extension of the threats, risks, and vulnerabilities that already exist with the terrestrial internet. Therefore, the threats, risks, and vulnerabilities usually related to the terrestrial Internet will not be discussed in relation to the threat analysis or risk assessment mentioned in this document, although a user need to be aware that they still exist.

A high-risk area in the context of this document is defined as a region or country where there exists one or several antagonistic parties with the intention of destroying, controlling, or shutting down ways of communication in order to sabotage opposing parties, control what media is distributed, or hinder the freedom of speech or freedom of the press. An

example of this would be a warzone or dictatorship.

The overview of threats, risks, and vulnerabilities associated with using satellite internet in high-risk areas, as well as the risk assessment, mitigations, and best practices presented in this guide, are based on the author's best knowledge and understanding of the subject matter and its basis in the sources that they have reviewed. It should be noted that the threats and risks can vary depending on the specific context and location.

Readers should be aware that the use of these satellite systems may be treated as illegal or punishable in some countries or regions where the governing nation or group is trying to silence opposing parties or suppress the freedom of speech. Therefore it may prove troublesome to get these devices into a country or region in a safe and discrete manner. This is however a legal matter which is not further discussed in this document.

This guide should not be considered a substitute for a professionally performed risk assessment or threat analysis by an experienced organization or company. It is meant to provide a starting point for informed decision-making about whether satellite internet is a viable option for communication in a high-risk area.

Readers should also be aware that the use of satellite internet in high-risk areas involves inherent risks and uncertainties, and it is the responsibility of the individual or organization to assess and manage those risks. The authors of this guide cannot be held liable for any loss or damage resulting from the use of the information provided herein.

Chapter 2

Satellite internet fundamentals

The purpose of this chapter is to provide the reader with some fundamental information about satellite internet systems. Here we will explain the different parts of the satellite networks infrastructure, how satellite internet systems operate as well as how they tie in to and differ from terrestrial internet infrastructure. This chapter will also give a small overview of some common satellite internet shortcomings.

2.1 Satellite internet infrastructure

The infrastructure of satellite-based internet consists of three main components: the user equipment, the satellite, and the ground segment. The user equipment includes a dish antenna, a modem, and a router which is installed at the user's location. The ground segment includes the Internet Service Provider (ISP) ground station and their gateway to the Internet backbone. The satellite itself relays signals with radio waves between the user equipment and the ground segment [4].

There are two main types of satellites used for internet connectivity, which are Geostationary Earth Orbit (GEO) satellites and Non-Geostationary Earth Orbit (NGEO) which are further subdivided into Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellites. GEO satellites are positioned at a fixed position, in a location above the earth's equator about 36000 km above the earth. This gives them coverage of about a third of the earth's surface when sending and receiving signals, while NGEO satellites orbit the earth at a much lower altitude. MEO satellites sustain their orbit at an altitude of about 2000 km above the surface, up to the height of GEO satellites, and LEO satellites sustain their orbit on an altitude of around 200-2000 km. LEO - satellites move relative to the earth's surface and therefore need a constellation of a large number of satellites in order to provide continuous coverage. The same is true for MEO-satellites that occupy the middle ground between LEO and GEO - satellites in that they also need a constellation of satellites to gain full coverage of the earth, but they do not need as many [3].

2.2 Satellite vs Terrestrial internet

The most significant difference in satellite internet is its use of long-range radio waves for communication and connectivity compared to the terrestrial internet which utilizes cables in some form for connectivity, usually copper or fiber-optic. The terrestrial internet is limited to areas where the cables can reach, a limitation that satellite internet does not have[4].

One of the main advantages of satellite-based internet over terrestrial internet is its global coverage. As long as the user has a clear line of sight to the satellite, they can access the internet from virtually anywhere on the planet. This makes it a valuable tool for disaster response and recovery, as well as for providing internet access to remote or under-served communities. However, satellite-based internet also has some limitations,

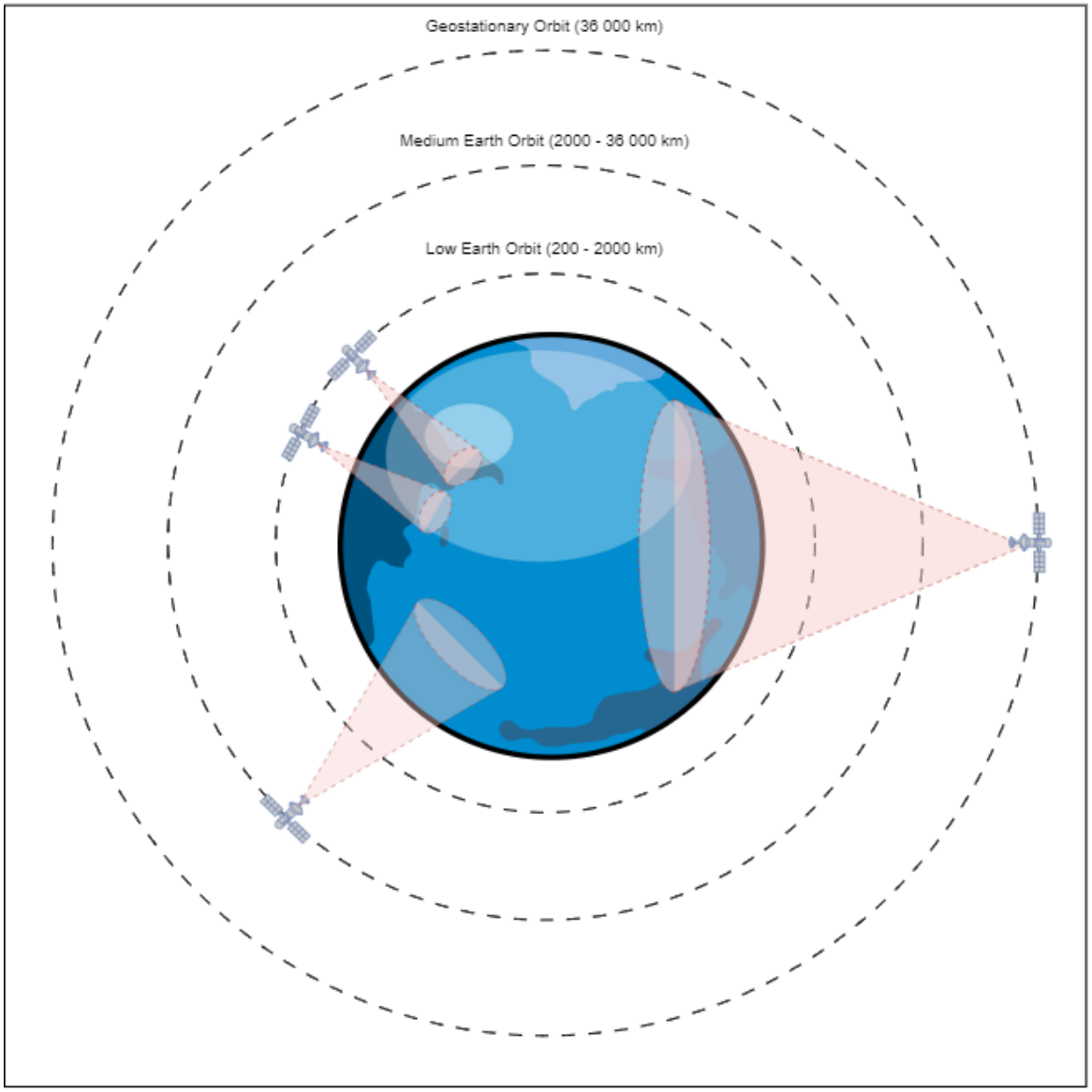

Figure 2.1: Illustration of different satellite orbits

such as higher latency (delay) and lower bandwidth (data transfer rate) compared to terrestrial connections, due to the long distance that signals have to travel between the Earth and the satellite[4].

LEO satellites however have some advantages over GEO satellites, such as lower latency and higher bandwidth, due to their closer proximity to the Earth. However, since LEO - satellite systems require a larger number of satellites, and the satellites need to move at very high speeds to remain in orbit, it makes it more difficult to track them in order to maintain a stable connection. Nonetheless, LEO satellite internet providers are emerging as a competitive alternative to traditional internet services in some areas, especially where the geography makes it difficult to lay

cables or erect cell towers[6].

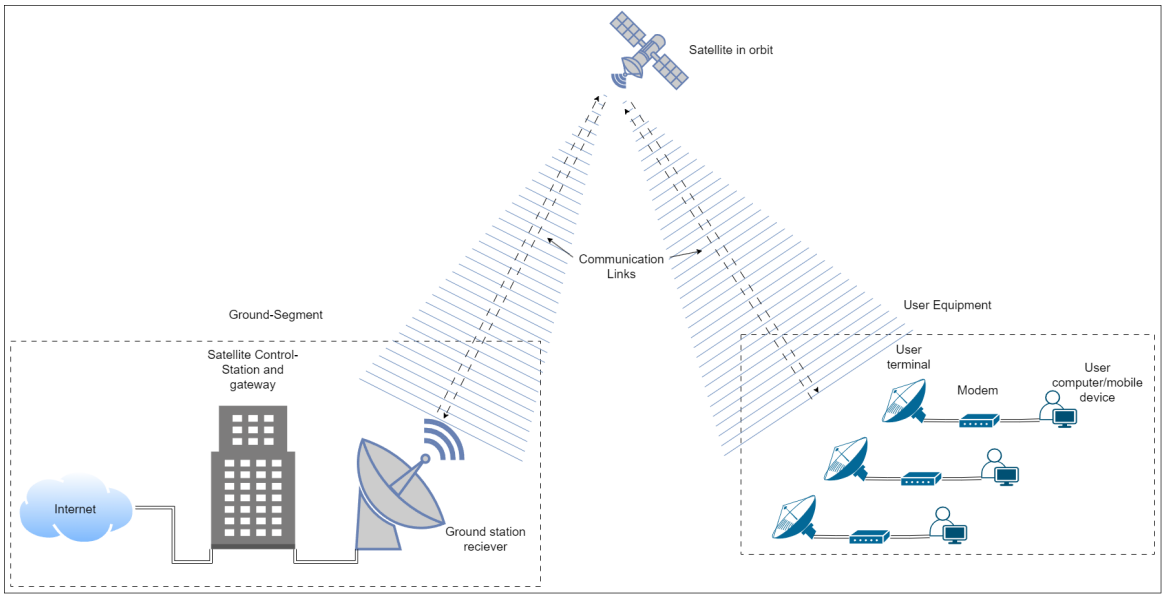

Figure 2.2: A basic view of satellite internet infrastructure

2.3 How the satellite internet system operates

The process of transmitting data over satellite-based internet begins with the user's request for a web page or other online resource. The user's dish antenna receives the request and transmits it to the satellite, which relays it to the ISP's ground station. The ground station processes the request and retrieves the requested data from the internet backbone. The requested data is then transmitted to the satellite, which relays it to the user's dish antenna. The modem and router in the user's equipment then decode the data and distribute it to the user's devices [3].

2.4 Satellite internet security shortcomings

Satellite internet has some security shortcomings that users should be aware of. One major issue is the weak or no encryption in the communication link. Due to the latency of satellite internet and the limited resources that can be applied in satellites, satellite providers often substitute security for performance. This can leave users vulnerable to eavesdropping and other types of attacks.

Another issue is the weak authentication of the satellite network, which is also due to limited resources. In some cases, the authentication process may be easily bypassed, allowing unauthorized access to the network.

In addition, the protocols used in satellite internet are not always secure. Some of the internet protocols of the terrestrial internet are not suited for use in satellite internet, therefore satellite internet uses lighter versions of these protocols that make a compromise between security and performance. This can result in the use of insecure protocols, which can leave users vulnerable to attacks.

Finally, there is the issue of poor physical security. It is relatively easy to interfere with the signals of the network through jamming and eavesdropping, for example. This means that the confidentiality and integrity of data transmitted over satellite internet may be compromised [5, 7, 2, 8, 9, 10, 1].

The threats that are related to these issues as well as other security threats will be discussed in the following chapters.

Chapter 3

Common threats and risks

When deciding on whether to utilize satellite internet or not, it is important to be aware of what the threats are and what impact they could have. In this chapter, the aim is to present to the reader what threats exist and how they manifest within the context of satellite internet. In the former chapter, an example of the infrastructure of satellite communication was shown, and from this, we can see what parts an attacker may target.

3.1 Targets of attack

With the information given in Chapter 2 and in figure 2.2, we can identify what targets of attack an attacker may choose from. The targets are the user station, the satellite, the ground station, and the communication links between the satellite and user stations as well as between the satellite and the ground station.

3.2 Threats and their consequences

With the targets of attack identified, we can now take a look at what the actual threats are when using satellite internet.

Eavesdropping is an attack that targets the communication link of the satellite infrastructure. It can be performed by an attacker aiming specialized equipment at the satellite and recording data being sent via the communication link. This type of attack is relatively easy to perform and if the data being sent is not encrypted it can lead to information disclosure. This means an attacker could for example read any emails being sent or see what web pages the user visits. Important to note is that depending on the capability of the attacker they may even be able to break the encryption that is used.

Replay attack is when an attacker first uses eavesdropping to record a message being sent and later resends the same message. Depending on the message being sent this could lead to the attacker being able to impersonate the user who sent the message, or perform unwanted actions on behalf of the user who sent the message. This type of attack is slightly more complex than simply eavesdropping as it also requires the attacker to find and resend a desirable message.

Hijacking is an attack in which an attacker gains control of, for example, a satellite. In this case, the attacker may be able to deorbit or otherwise sabotage the satellite in order to cause a loss of connection to the users. The attacker may also be able to eavesdrop on all data being sent via the satellite. This type of attack is very complex as it requires the attacker to possess significant knowledge of the inner workings of the satellite, as well as gaining access to it presumably from the control center which is used by the service provider to control and manage their satellites.

Jamming is an attack that targets the communication link of the satellite communication. This type of attack involves an attacker using

specialized equipment to produce a strong signal which drowns out the legitimate signal of the user, causing a loss of connection. The loss of connection is however temporary and if the attacker turns off the jamming device connection is restored. This type of attack is not very complex as it only requires specialized equipment and it is often used by parties of the conflict in a warzone.

Message modification is an attack similar to the replay attack, but here the attacker modifies the original message in some way to produce illegitimate results. As the original message is altered it would require the attacker to intercept and suppress the original message while resending the modified message. This attack could lead to the attacker modifying an email being sent, gaining illegitimate access meant for the user, or performing unwanted actions which can be traced back to the original user instead of the attacker. This type of attack is relatively complex in comparison to the replay attack as it requires the attacker to not only intercept the message but also modify and suppress it before resending it.

Malware is malicious software an attacker installs on a device that then performs an unwanted action. For example, this action could be sabotaging the device so that it no longer functions properly, or stealing data from the device. In the context of satellite infrastructure malware could infect all parts of the network except the communication links as these are not devices. This type of attack differs in complexity depending on what the target is. The ground station and user station consist of devices that would be similar or the same as devices used in terrestrial communication, meaning malware affecting these targets would not need to be as complex as malware affecting the satellite itself, as this would most likely require specialized knowledge.

Tracking is when an attacker is able to gain the location of a user. The user station and satellite use radio waves to communicate with each other, and these radio waves can be used to track the user station. While tracking the radio waves emitted from the user station would require specialized equipment its complexity can be likened to jamming. It should be assumed that the user station always emits radio waves when it is turned on.

Chapter 4

Risk assessment

The aim of this chapter is to present a simple risk assessment of the threats that have been mentioned to give the reader a better understanding of how they may be impacted. As risks can be interpreted differently depending on the context, what considerations that are made, and the perspective of the risk assessment, it is important to note that the reader may experience the risks differently. This risk assessment should therefore only be seen as an example that may or may not apply to the reader.

To evaluate the risk of the threats a generic risk calculation is used in this document. This is a simple formula that is defined as "$Risk = Probability * Impact$", and it gives a score for each threat based on the probability of the threat happening, and what impact the threat will have if it happens.

The probability score and impact score in our calculation range from 1 to 5 and since the risk score is a product of these it ranges from 1 to 25. A probability score of 1 means the threat is not likely to happen, and a score of 5 means it is almost guaranteed to happen. An impact score of 1 means the threat has a temporary disruption and does not affect the safety of the user, while a score of 5 means the personal safety of the user is threatened. In Figure 4.1 a visual representation of the risk score is presented, and as an example, probability score of 5 and impact score of 5 would land on "Unacceptable risk".

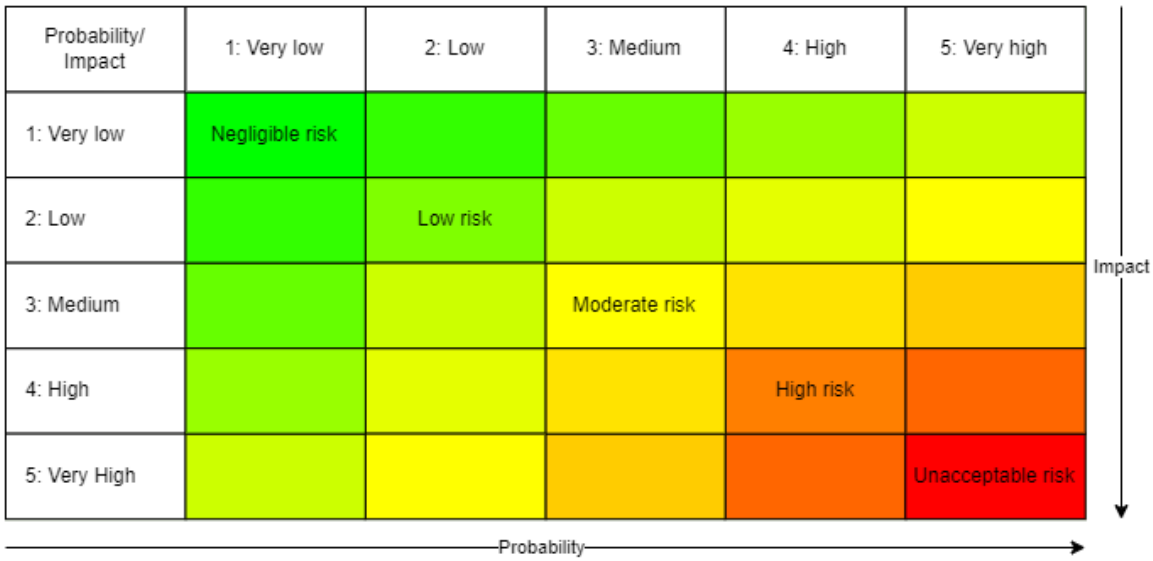

Figure 4.1: An illustration of the risk-spectrum

1. Negligible Risk: The risk is minimal and can be accepted without any significant concern.

2. Low Risk: The risk is low and can be accepted with some level of confidence.

3. Moderate Risk: The risk is moderate and requires some attention and management to minimize its impact.

4. High Risk: The risk is high and needs immediate attention and management to reduce its impact.

5. Unacceptable Risk: The risk is very severe and cannot be accepted under any circumstances.

4.1 What is the perspective?

The risk assessment was made from the perspective of a fictional civilian located in a high-risk area. A high-risk area in this context is defined as an area in which there are ongoing hostilities, such as a war or ongoing government oppression. The civilian is a journalist reporting on the events in the area and is using satellite internet communication to send their reports back to their company headquarters. This means that the civilian may be sending sensitive material which they do not wish to be intercepted as it may lead to an adversary threatening their personal safety. For this reason, they also do not wish to disclose their current location in any way.

4.2 What are the risks?

Below the assessment of each threat is presented along with an explanation for their scoring. Keep in mind these scores are given from the perspective stated in the former section. Since probability and impact will vary depending on the region and situation in which satellite internet is intended to be used, the risk assessment presented below should not be applied to a real situation. It is only presented to provide the our reasoning for the scenario stated in the previous section.

Hijacking

Probability score: 1
Explanation: For an attacker to perform this action they need to access the satellite in some way. The most likely target is the ground control station which then could give the attacker access to the satellite. However, the attacker would need intimate knowledge of the satellite architecture.
Impact score: 4
Explanation: The attacker is able to read and potentially modify all data being sent via the satellite. There is also a potential for the attacker to control the satellite and for example, deorbit it.
Total score: 4

Jamming

Probability score: 5
Explanation: Jamming devices can be very easily implemented and utilized by an attacker , due to the low cost and complexity of implementation and deployment.
Impact score: 1
Explanation: This could lead to the connection being dropped altogether. This is however a temporary disruption as when the jamming devices is turned off or targeting other frequencies the connection is restored.
Total score: 5

Replay attack

Probability score: 4
Explanation: An attacker needs to be able to record messages being sent as well as send them at a later time. This requires some technical know-how but its relative complexity is low.
Impact score: 2
Explanation: The impact depends on the message resent, but it could result in an attacker being able to impersonate a real user. This could lead to the disclosure of sensitive information and even the elevation of privilege for the attacker.
Total score: 8

Malware

Probability score: 3
Explanation: The probability is medium here as there are known cases of malware infecting user terminals. The probability of ground stations can also be considered relatively high as this is terrestrial communication. For the satellite to be infected by malware however would require specialized software and know-how which makes it relatively complex.
Impact score: 3
Explanation: If the ground station is infected with malware it is possible that the connection is lost with the satellite. If the satellite gets infected all connections with that satellite could be lost and it could fall out of orbit. If the user station gets infected that user could lose their connection.
Total score: 9

Eavesdropping

Probability score: 5
Explanation: The probability of eavesdropping is high since it does not require too much knowledge of the satellite systems and fairly non-expensive equipment in order to be successful.
Impact score: 2
Explanation: May lead to accidental disclosure of sensitive information and data due to the transmission channel not being secure and allowing for eavesdropping.
Total score: 10

Message modification

Probability score: 3
Explanation: This requires the attacker to be able to intercept a message, alter the message and then resend the message to the receiver. The technical know-how involved is greater than that of a replay attack or simple eavesdropping since the attacker needs to be perceived as a legitimate user by the system.
Impact score: 4
Explanation: This could lead to an attacker gaining privileges they are not meant to have by for example altering the messages of a control message. The attacker could also take actions on behalf of the user which the user cannot deny as their message was used to perform these actions.
Total score: 12

Tracking

Probability score: 4
Explanation: An adversary uses the communication link to locate satellite user stations. The complexity is not that high to realize this threat, and nation-states are known to have these capabilities and use them in high-risk zones.
Impact score: 5
Explanation: If a user is utilizing satellite internet in a potentially hostile area, the user may unintentionally make themselves a target of antagonistic forces interpreting their signal as an adversary trying to communicate. Additionally, a user may be tracked by government actors who seek to silence or incarcerate the user of the satellite internet con-

nection.
Total score: 20

4.3 Threats in relation to the CIA-triad

The CIA-triad is a widely recognized model for information security that stands for Confidentiality, Integrity, and Availability. In Figure 4.2 a visual representation of this model is presented. Here is a brief explanation of each attribute:

- **Confidentiality:** Refers to the protection of information from unauthorized access or disclosure. It involves keeping sensitive information private and ensuring that it is only accessible to authorized individuals.
- **Integrity:** Refers to the accuracy and consistency of information. It involves ensuring that data is not modified, deleted, or tampered with in any way by unauthorized individuals. Maintaining data integrity is essential for ensuring the trustworthiness and reliability of information.
- **Availability:** Refers to the ability to access information when it is needed. It involves ensuring that information is available to authorized users at all times and that it can be accessed quickly and reliably. Maintaining availability is crucial for ensuring that critical systems and services are always up and running.

Figure 4.2: A figure representing the CIA-triad with each key attribute in a corner of a triangle.

In Table 4.1 the threats that were found and what attribute of the CIA-triad they affect are presented. Hijacking, message modification, eavesdropping, malware, and tracking affect the confidentiality of the system. Replay attacks, hijacking, message modification, and malware affect the integrity of the system. Hijacking, jamming, and malware affect the availability of the system.

Threat	Confidentiality	Integrity	Availability
Replay attack		A replay attack can affect integrity by allowing attackers to replay old data and overwrite or manipulate current data, leading to the spreading of false or inaccurate information.	
Hijacking	Hijacking compromises confidentiality because attackers gain access to the communication channel and can intercept sensitive, confidential information.	Hijacking can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	Hijacking can impact availability by denying users access to critical resources. For example, if an attacker hijacks a communication channel during an emergency, it can prevent first responders from accessing important information.
Message-modification	Message modification compromises confidentiality because attackers can access and modify sensitive, confidential information.	Message modification can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	
Eavesdropping	Eavesdropping compromises confidentiality because attackers can intercept and access sensitive, confidential information.		
Jamming			Jamming can impact availability by blocking or disrupting the communication channels used by the satellite, thereby denying users access to critical resources during the use of the satellite systems.
Malware	Malware can compromise data confidentiality by potentially collecting and sending sensitive data to an attacker.	Malware can affect integrity by allowing attackers to modify or replace original data which may lead to the spreading of false or inaccurate information.	Malware can impact availability by causing delays in data transmission, affecting network performance, and potentially shutting down the system, which can have severe consequences in an emergency.
Tracking	Tracking can compromise the confidentiality of data, which can be particularly dangerous in a high-risk zone where sensitive information must be kept secure., It exposes the location of the users to the attackers, which can put them in danger.		

Table 4.1: Table showing the relation between the threats and Confidentiality Integrity and Availability (CIA)

Chapter 5

Mitigations and best practices

In this chapter, we discuss the different mitigations a user can apply to decrease the probability and impact of the risks mentioned in the previous chapter. The aim is to provide the user with knowledge of what security measures can be applied by them in the context of satellite internet, and what threats they affect.

5.1 Mitigating the threats

The first mitigation to consider is the use of encryption. A type of encryption often used is Virtual Private Network (VPN). A VPN works by encrypting the data sent between two points in a network, adding a layer of security to the connection. As VPN encrypts the data being sent, it reduces the risk of an attacker gaining access or modifying the data being sent. This means that of the previously mentioned threats it mitigates eavesdropping and message modification. While using VPN does not stop the ability of an attacker to perform a replay attack, it lowers their ability to determine what message would be desirable to resend. It is also important to note that satellite internet providers use a technique called performance-enhancing proxies to increase the performance of satellite internet, and when utilizing VPN this technique might not work which means that the connection can become very slow.

The second mitigation is to keep all devices up to date. When a vulnerability is discovered, an update to fix this vulnerability may be released by the manufacturer of the device, which means that keeping a device's security updates up to date, such as the user station, helps mitigate risks where an attacker may try to exploit a known vulnerability. This mitigation helps against being infected by malware and an attacker gaining access to the user's device.

Three of the threats have not yet been addressed, these are hijacking, jamming, and tracking. When it comes to hijacking there is very little the user can do in terms of mitigation. The user can still use secure tunneling to protect their data but the responsibility for this risk is on the service provider. Jamming is a threat due to the wireless connection of satellite internet and is not a threat that the user themselves can mitigate. The impact of this threat is also not as severe as the others due to it only affecting the availability of the connection, as well as being temporary.

Tracking is a threat in which the mitigation is user awareness and using the connection in a responsible way. The user station may be tracked through its radio emission and the user cannot affect this, the only guarantee to not be tracked is turning off the user station and removing any power supply, such as batteries. It is therefore important that the user knows this and use the connection only when it is necessary, to for example sending an important email, then turn it off and change location after it has been used. The connection should also not be used in places where the user is frequently located, such as their hotel room or similar locations.

Threat	CIA attribute affected	Mitigation
Eavesdropping	Confidentiality	Encryption
Tracking	Confidentiality	Turn off the terminal
Jamming	Availability	No available mitigation
Message modification	Confidentiality, Integrity	Encryption
Replay attack	Integrity	Encryption
Hijacking	Confidentiality, Integrity, Availability	Encryption
Malware	Confidentiality, Integrity, Availability	Install security updates

Table 5.1: The threats in connection to the CIA attributes they affect and what mitigations can be utilized against the threat.

Table 5.1 shows a summary of the different threats in relation to the CIA-triad and the mitigations for each threat.

5.2 Recommended best practices

There are some best practices that a user should consider when utilizing satellite internet communication in a high-risk area:

- **Limit usage:** It is important to use the connection only when necessary to send sensitive information and encrypt the communication. One can also employ some type of predetermined coded language for extra security. Excessive usage can attract attention and increase the risk of being detected. The device should always be powered off when not in use.
- **Keep the device secure:** It is essential to keep the device in a safe and secure location when not in use. It should be locked away in a secure place to avoid unauthorized access.
- **Being tracked is an inevitability:** The user must understand that by just using the device they can attract unwanted attention. Use the device in a way that it cannot be traced back to their home or hideout. Use the device with the assumption that as soon as it is powered on it will be tracked, and turn it off when not in use.
- **Employ standard best practices for secure internet usage:** Besides the above-mentioned best practices for using satellite internet safely and securely, the same best practices that a user would employ for safe and secure use of the terrestrial internet should still be employed when using satellite internet. These include but are not limited to:

- Use strong passwords for each account which include a combination of upper and lowercase letters, numbers, and symbols. Avoid using common words or phrases that can be easily guessed.
- Keep your operating system, web browser, and antivirus software up-to-date with the latest security patches and updates.
- Use antivirus software to protect your computer from malware and other threats. Ensure that it is updated regularly to stay protected against the latest threats.
- Use a firewall to block unauthorized access to your computer or network.
- Be cautious when opening emails from unknown senders or with suspicious attachments. Avoid clicking on links in emails unless you are sure they are legitimate.
- Use secure websites: Look for "https" in the URL to ensure that it is a secure connection. Avoid entering sensitive information on websites that do not have "https" in their URL. This is because if the website is using only the "http"-protocol the information sent to the website is not encrypted.
- Be cautious when sharing personal information on social media. Avoid sharing sensitive information such as your home address, phone number, or date of birth as it can be used to launch an attack against you.
- Back up your important data regularly to ensure that you do not lose it in case of a cyber-attack or other disaster. Also, keep your backups secure and isolated since they could contain sensitive data.

Bibliography

[1] H. Cruickshank, L. Liangl, P. Pillai, M. Noisternig, B. Collini-Nocker, and G. Fairhurst, "Unified link layer security design for ip encapsulation using unidirectional lightweight encapsulation over satellites," in *IET Conference Publications*, 2009. [Online]. Available: https://doi.org/10.1049/cp.2009.1153

[2] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 1, pp. 53–87, 2022. [Online]. Available: https://doi.org/10.1109/COMST.2021.3131332

[3] Y. Hu and V. Li, "Satellite-based internet: a tutorial," *IEEE Communications Magazine*, vol. 39, no. 3, pp. 154–162, 2001. [Online]. Available: https://doi.org/10.1109/35.910603

[4] M. K. Iqbal, M. B. Iqbal, S. Shamoon, and M. Bhatti, "Future of satellite broadband internet services and comparison with terrestrial access methods e.g. dsl and cable modem," in *2013 3rd IEEE International Conference on Computer, Control and Communication (IC4)*, 2013, pp. 1–5. [Online]. Available: https://doi.org/10.1109/IC4.2013.6653763

[5] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *International Journal of Information Security*, vol. 20, pp. 287–311, 2021. [Online]. Available: https://doi.org/10.1007/s10207-020-00503-w

[6] T. Matus. (2021) Starlink vs. standard broadband: How do they compare & which is better? [Accessed March 30, 2023]. [Online]. Available: https://history-computer.com/starlink-vs-standard-broadband-how-do-they-compare-which-is-better/

[7] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband," in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 277–284. [Online]. Available: https://doi.org/10.1145/3317549.3323418

[8] J. K. Pedersen, M. Bochman, and W. Meng, "Security analysis in satellite communication based on geostationary orbit," in *2022 19th Annual International Conference on Privacy, Security and Trust, PST 2022*, 2022. [Online]. Available: https://doi.org/10.1109/PST55820.2022.9851962

[9] J. M. Rodriguez Bejarano, A. Yun, and B. De La Cuesta, "Security in ip satellite networks: Comsec and transec integration aspects," in *2012 6th Advanced Satellite Multimedia Systems Conference, ASMS 2012 and 12th Signal Processing for Space Communications Workshop, SPSC 2012*, 2012, pp. 281–288. [Online]. Available: https://doi.org/10.1109/ASMS-SPSC.2012.6333089

[10] X. Wu, Y. Du, T. Fan, J. Guo, J. Ren, R. Wu, and T. Zheng, "Threat analysis for space information network based on network security attributes: a review," *Complex and Intelligent Systems*, 2022. [Online]. Available: https://doi.org/10.1007/s40747-022-00899-z

Faculty of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden