South-Eastern Finland
University of Applied Sciences

Ashkan Abdulla Mohammad

Starlink Internet Services

Starlink Internet services and its security aspects

Bachelor’s thesis

Bachelor’s degree of Engineering

Information Technology

2023

South-Eastern Finland
University of Applied Sciences

Degree title: Bachelor’s degree in information technology

Author: Ashkan Abdulla Mohammad

Thesis title: Starlink Internet Services

Year: 2023

Pages: 40 pages

Supervisor: Matti Juutilainen

ABSTRACT

As Starlink takes its place as one of the leaders in the satellite internet sector, concerns are being raised about the potential vulnerabilities and security challenges inherent in such an interconnected system. This paper identified and addressed the security aspect in Starlink services since it is important to ensure the security and privacy of customers using these services. This research used a literature-based methodology, using past articles that review and examines the security aspects of Satellite internet constellations, with some focusing on Starlink. Analysis of Starlink security shows issues such as the vulnerability of cyber threats and the possibility of abuse of surveillance, is supported by case studies such as the Ukraine conflict and related Starlink router vulnerabilities. This paper also identified that there are legal challenges around Starlink's global operations meaning that international cooperation and transparent policies are needed. Even so there are measures put in place by Starlink to safeguard their system. Integration of encryption and authentication protocols, automation, and autonomy in satellite systems, user privacy protection, and active user education programs all combine to support Starlink’s security system.

Keywords: Starlink, Satellite-based Internet, security

challenges, cyber threat

CONTENTS

LIST OF FIGURES

1 INTRODUCTION

High-speed technology is rapidly changing the way we live. A great example is how the internet has spread through smartphones, opening up new possibilities for many people. According to Shaengchart et al. (2023), this ongoing change is called "Industry 4.0," and it's quickly transforming the economies and societies. Different ways of using technology are evolving really fast, both inside and outside of businesses. Many countries are strategically positioned to embrace new ways of doing things because of the mix of economic, social, and technological forces coming together. This change is affecting the traditional ways we buy and sell things. In developed countries, important sectors like finance, housing, healthcare, social security, and mobility are shifting from physical places to online platforms. Big data, Internet of Things (IoT), cloud computing, and artificial intelligence (AI) are greatly impacting every part of society. The economy depends on digital technology because it depends on services. Undoubtedly, the Internet is a monumental technological advancement in human history, now integral to daily life. Today, common broadband technologies like xDSL and cable modems are giving way to the superior performance of optical fibres. While fibre deployment proves profitable in bustling urban hubs, it becomes a pricier challenge in remote or mountainous regions. A good option to provide internet to these areas is by “internet from space”. In today's world, space is more than just the huge area above us. Thummala (2023) highlights its significance in supplying energy for things like power grids, financial transactions, GPS, telecommunications, weather forecasts, and air travel.

This paper is about Starlink which is a satellite Internet constellation operated by private aviation and space company SpaceX. They started giving internet in 2020 in the U.S. and later in Europe, Starlink has one of the biggest setup with over 2,000 satellites in space (Michel et al., 2022). The internet they provide is super-fast, with low delays and speeds between 100 to 200 megabits per second (Michel et al., 2022). As Starlink becomes a top player in satellite internet, people worry about possible weaknesses and security issues in its big, connected system. The objectives of this research is to understand how Starlink satellite internet service works, and identifying potential security issues and weaknesses in Starlink as well as evaluating how well Starlink’s current security measures protect against potential risks.

In addition to the objectives, the study aims to answer the following questions:

a) How does the system for Starlink satellite internet service work to provide global connectivity?

b) What security challenges and vulnerabilities exist within Starlink's network infrastructure?

c) How effective does Starlink implement the existing security measures in safeguarding against potential risks and ensuring the integrity of data transmission?

2 LITERATURE REVIEW

There has been advancement since the idea of Satellite internet first emerged. This chapter is going to talk about the history of Satellite internet, reasons why it was not popular, the security set up and the history of SpaceX. Finally this chapter will look at case studies where there has been use of satellite internet and the impacts.

2.1 History of Satellite-Based Internet

Over the past ten years, new satellite internet companies globally have emerged, joining the traditional internet connections through fiber-optic cables. Companies like O3B, SpaceX, and OneWeb have big plans to bring internet access to people all around the world, especially those in underserved areas (Graydon & Parks, 2020, p. 2). Looking back at the start of this satellite internet trend, Gerber (2023) points out that Iridium was the pioneer, achieving internet access through Low Earth Orbit (LEO) satellites in 1998 (p. 45). Iridium had a group of 66 satellites orbiting close by and provided speeds of 2.4 Kb/s. Originally designed for satellite phones, the slow speeds limited its data capabilities. To improve speed and reduce latency, Iridium used satellite relays and ground stations, making it faster than satellites in Geostationary Orbit (GEO) (Gerber, 2023, p. 46). Iridium, despite its technological prowess, had financial problems and went bankrupt in 1999. High launch costs, problems with the circuits, and high maintenance costs were considered to be the main cause of their failure (Gerber, 2023, p. 46). It came back in 2001 with new owners, but had issues because the old satellites weren't working well. Even though it kept going until 2017, it wasn't as effective.

Globalstar started operating in February 2000, offering satellite phone services and trying out internet provision. Similar to Iridium's goal, Globalstar focused mainly on satellite phones, with additional internet access at a speed of 9.6 kilobits per second for users (Gerber, 2023, p. 46). This technology relied on a group of 48 satellites orbiting at a height of 1,414 kilometers (Gerber, 2023, p. 46). However, despite its ongoing use, Globalstar faced money problems and filed for bankruptcy in 2003. The financial challenges were due to high operating costs and a limited number of users, leading to a reorganization (Gerber, 2023, p. 46). The troubles faced by both Iridium and Globalstar highlighted concerns raised by critics of Low Earth Orbit (LEO) constellations during that time. The need to deploy hundreds or even thousands of satellites for worldwide coverage was costly, and there wasn't enough demand for services, resulting in the early closure of these pioneering companies.

Back in the early days of the satellite internet, there was a big problem. The people creating it had a hard time because the speed of connection was much slower than what regular internet providers on land offered, which could go up to 56 kb/s (Gerber, 2023, p. 46). But in 2004, something changed, a special satellite with powerful technology called Ka-band was sent into space, this made the internet much faster (Gerber, 2023, p. 46). Companies like Viasat and Wildblue used this opportunity to offer internet that was as fast as the kind you get from cables on the ground, this was all thanks to these new and innovative GEO satellites (Gerber, 2023, p. 46).

Advancements in satellite technology have led to the widespread availability of internet access, this progress gained momentum through a series of successful launches of similar technology. GEO satellite internet access has become a reality, reaching places beyond the scope of traditional services on Earth (Gerber, 2023, p. 46). Although the Ka-band had been used in Low Earth Orbit (LEO) satellites in the 2000s, it wasn't until 2017 that companies boldly embraced large-scale LEO satellite internet access. This era gave rise to innovative constellations like Kuiper, Starlink, Telesat, and OneWeb (Herath, 2021). Each is charting their own course by utilizing advanced technologies in spectrum usage, satellite capabilities, ground equipment upgrading, and systems management. Among them, Starlink has emerged as a leader, making significant progress in reaching more areas and advancing towards full-scale deployment (Herath, 2021).

2.2 Why Satellite Internet was not popular

Unlike traditional TV broadcasts that only send information in one direction, the way the satellite Internet works involves a back-and-forth exchange of data. For this to happen, it requires installing special satellite dishes to send and receive data. This setup adds complexity and brings challenges like cost, capacity, and delays, creating an unsatisfactory experience for users. Comparing this to regular cable broadband, satellite connections were harder to set up and cost more to maintain, as pointed out by Graydon and Parks (2020). When launching satellites to provide Internet to many users, providers need to carefully manage how they share the available data. This might involve putting limits on how much data each user can use, especially with data-heavy activities like streaming high-quality videos.

Among all types of satellite internet services, latency is a major obstacle that needs attention (Graydon & Parks, 2020, p. 5). Latency is the time delay between sending and receiving data. Unlike the conventional Internet, satellites share additional resources because they are far away in space, and data must travel long distances at the speed of light. In most satellite Internet, this delay is around 500–600 milliseconds (Graydon & Parks, 2020, p. 5). This delay doesn't matter much when watching TV, but it causes issues with other things like browsing the Internet or streaming videos. Sometimes, content takes a while to load, causing annoying delays. This is especially noticeable in activities like playing online games, using Skype, watching live streams, and using social media (Graydon & Parks, 2020, p. 5). These are services that became popular in the early 2000s when broadband Internet started. People who are used to fast broadband were disappointed with the delays in satellite Internet. This was a problem for companies that provided satellite Internet, as a result they were not be able to compete well with other Internet providers.

From 2000 to 2010, a lot more folks in places like the United States began using home broadband. The percentage of users jumped from only 1% to a whopping 61%, as per a 2018 report by the Pew Research Center, this showed a quick increase in the popularity of cable broadband connections (Graydon & Parks, 2020, p. 5). However, this growth had a downside for satellite Internet services. While using satellites for internet was expensive and took a lot of time, laying underground and undersea fiber optic cables turned out to be a more cost-effective option (Graydon & Parks, 2020, p. 5). It was a better choice than the costly processes involved in creating, launching, and maintaining satellite-based communication systems. Apart from being more economical, the land-based systems had advantages like quick repairs, upgrades, and expansion to meet the changing needs of users (Graydon & Parks, 2020, p. 5). This empowered local and national businesses and their workforce. As a result, fiber optic cables became the preferred infrastructure for internet traffic in many parts of the world.

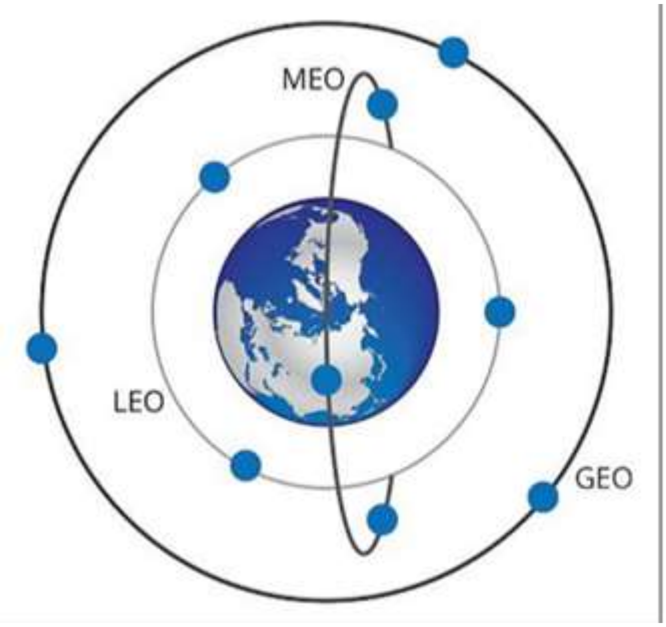
Despite challenges, a few telecommunications experts were very hopeful about satellite technology. One of them was Craig McCaw, who supported the groundbreaking idea for a satellite Internet system in 1990. He aimed to overcome speed and cost issues that held back the widespread use of this technology. McCaw started a company called Teledesic with the bold goal of providing global, high-speed Internet using 840 satellites in Low Earth Orbit (Graydon & Parks, 2020, p. 5). Sadly, Teledesic faced insurmountable challenges, mainly due to the massive cost of building such an extensive satellite network, which exceeded the billion-dollar venture capital the company had.

Telecommunications Experts, especially the critics, raised questions about whether the project made sense in the market. After Teledesic's failure, the idea of a global satellite internet network became less important in the world of telecommunications (Graydon & Parks, 2020, p. 6). Instead, huge amounts of money were being invested in building internet infrastructure on land. Companies decided that spending money in laying thousands of kilometers of cables across continents and under the ocean was worth than investing in Satellite internet. Satellite internet started to play a more specialized role, mainly serving the needs of industries, governments, and the small number of people living in remote rural areas where regular broadband was not available. One area where satellite internet services saw significant growth was in the travel industry, especially in commercial air and cruise lines. According to Graydon and Parks (2020, p. 6), a remarkable two-thirds of airlines plan to offer in-flight internet via satellite. Major cruise lines also provide satellite internet, although there may be challenges like slower speeds and higher costs when many people are using it at the same time due to limited available bandwidth for the entire ship.

2.3 Satellite Internet Revolution

Traditional satellite communication uses GEO satellites far away in the sky, about 35,771.14 kilometers from Earth. While one satellite can cover a big space, its high location causes delays, making the internet slower with delays of hundreds of milliseconds. Mitchell et al. (2022) talk about a communication tech that helps thousands at speeds up to 100 MB. But, there's a delay of at least 600 ms. These Medium Earth Orbit (MEO) satellites are not too close or too far, just around 2,000 to 35,786 kilometers above Earth (Coughlin, 2023, p. 5). They're good because they provide wide coverage and fast communication. These satellites are especially useful for navigation systems and special communication services. On the other hand, Low Earth Orbit (LEO) satellites are closer to Earth, around 160 to 2,000 kilometers high (Coughlin, 2023, p. 5). LEO satellites are becoming popular for modern satellite internet. They are super-fast because they're close, but we need more of them to cover as much as one GEO satellite, which stays much higher above Earth. Figure 1 shows the locations of three different satellites. Different satellites have different benefits depending on how high they are in the sky.

Figure 1: Representation of low, medium and geosynchronous orbits (Graydon & Parks, 2020)



The China Center for Information Industry Development (CCID) foretells that the skies will soon be packed with many satellites. They predict that around 57,000 low Earth orbit (LEO) satellites will be launched by 2029, starting a competition for space spots (Cao et al., 2020, p. 193). Using satellites in medium Earth orbit (MEO) for internet has potential because fewer satellites are needed than with low Earth orbit (LEO). However, LEO satellites outperform MEO ones because they give stronger signals and have less signal delay due to being closer to Earth (Kvant & Johansson, 2023, p. 7). LEO satellite internet has a few drawbacks. It doesn't cover as many places as regular satellite internet does, making it harder to get a connection in really faraway areas (Kvant & Johansson, 2023, p. 8). Also, the network isn't complete yet, so there might be times when it doesn't work well or stops working altogether. Fixing these issues is important as they work on finishing the network.

Satellite internet technology has evolved significantly, transforming the construction and performance of satellites. A major breakthrough involves making satellites smaller, especially in Low Earth Orbit (LEO) groups (Coughlin, 2023, p. 7). These compact satellites are a game-changer, as they are more cost-effective to build and launch compared to the larger, traditional ones. They leverage advanced materials and high-tech electronics to remain lightweight yet powerful (Coughlin, 2023, p. 7). The movement of satellites has improved too. The latest models feature more efficient propulsion systems, enhancing their longevity in space and ease of control (Coughlin, 2023, p. 7). This is vital for keeping satellites in their intended positions and preventing issues with space debris.

Additionally, there are noteworthy changes in how satellite networks are structured, contributing to the overall advancements in satellite technology. In the past, satellites mainly sent signals straight to ground stations. Now, there's a shift to creating links between satellites themselves (Coughlin, 2023, p. 7). This means satellites can talk to each other, forming a kind of network in space. This new setup makes satellite internet more reliable. If one satellite or ground station has issues, data can still find its way through other paths, making sure people stay connected all around the world. These improvements not only make satellite internet networks stronger but also help them provide consistent and reliable connections globally.

2.4 Security in Satellite Communications

The space industry has faced many challenges since it started. In a study by Cao et al. (2020), they explain the structure of the space industry in three main parts: the user, space, and ground segments (p. 195). Figure 2 shows a typical satellite components. The User Segment has gadgets to find where one is on Earth, like GPS devices that tell the exact location (Cao et al., 2020, p. 195). The space segment is all about the satellites, which can be in constellations with links between them (ISL) or without (Cao et al., 2020, p. 195). The third part is the ground segment, which has the gateway station (GS), operation management and control system (OMCS), measurement and control system (MCS), and network management system (NMS) (Cao et al., 2020, p. 195). All these parts work together to make the space industry function.

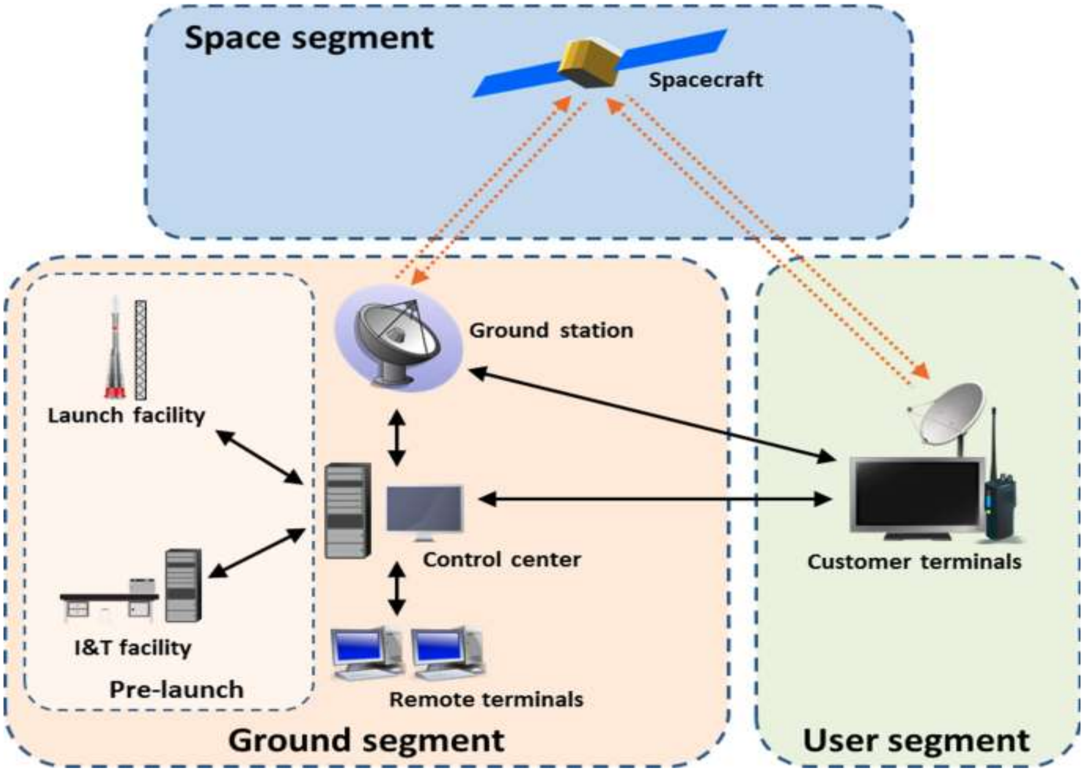


Figure 2: Typical satellite architecture (Manulis et al., 2021).

2.4.1 Ground Segment

Taking control of a satellite involves strategically compromising its ground station. This is because the ground station provides essential equipment and software for controlling and tracking the satellite. Cao et al., (2020) tells us to think of ground stations as the command centers for satellites, using existing systems on Earth (p. 203). Just like regular computers, these ground stations are vulnerable to network threats (Cao et al., 2020, p. 203). Attacking a satellite isn't as simple as stealing emails, but it's doable. Determined intruders can break into ground stations by finding security weaknesses. Once inside, they can send harmful commands to control the satellite or use special tools to deceive and manipulate it (Cao et al., 2020, p. 204). This can lead to an attack on the entire satellite system. Attackers can also use a targeted satellite's broadcast channels to spread fake data or viruses, expanding their impact. The aftermath of satellite control is up to the attacker's creativity: they can cause shutdowns, change the satellite's orbit to collide with other things in space, like other satellites or even the International Space Station (Cao et al., 2020, p. 204). Ground stations play a role in shaping how things move in space.

Satellite ground stations face ongoing threats that can harm their functioning. These threats come in different forms, with physical attacks being a major concern. Breaking into ground stations or other facilities is a physical attack that breaches security. Unauthorized access, as noted by Manulis et al. (2021), poses a serious threat to these stations and IT assets. Exploiting vulnerabilities in such attacks can activate ground stations, directly affecting mission operations and services. There's also a risk that determined enemies might take control of the satellite for their own malicious purposes. For example, in 2015, the Russian group Turla used a ground antenna to intercept communication between ground stations and geo-satellites, allowing them to access user information and engage in cyber espionage activities (Gerber, 2023, p. 5).

Computer community exploitation (CNE) can be any other example of an attacker successfully infiltrating a network tied to a ground station, as defined by means of Manulis et al. (2021). Attackers can use hints from hacking corporate computer structures to interrupt into ground stations. These hints contain taking benefit of weak or effortlessly hacked technology and using phishing to trick humans. Ground stations, which manipulate satellites, depend upon cloud infrastructure. This means everything from storing data to processing it happens in the cloud. If the cloud system gets hacked, it can cause big problems for the ground stations. This could lead to denial of service, making it hard for the satellite to work properly (Manulis et al., 2021). Even major cloud providers like AWS and Google Cloud are at risk of being disrupted by attacks (Manulis et al., 2021). This is a big threat to satellite systems that need to work in real-time. So, it's important to protect the cloud infrastructure to keep satellite operations safe.

Attacks on terrestrial networks seamlessly extend their impact to satellite networks, as exemplified by fraudulent attacks on distributed denial of service (DDoS). Even though there has been improvements in security, Cao et al. (2020) states that enemies may use sophisticated computer programs to pretend they are lots of different satellite devices, making it hard for the real satellites to tell which requests are real and which are fake (p. 202). This messes up the satellite system, and real users can't get the services they need (Cao et al., 2020, p. 202). It's tough to stop these attacks because satellites have a communication setup where each receiver works independently. If something goes wrong with one receiver, there's a mix-up in communication, especially when there are too many requests (Cao et al., 2020, p. 202). Also, when the weather is bad, more people try to connect to satellites, making the problem worse. The satellites struggle to tell the difference between normal connections and attacks, leading to a situation where real users can't get the services they need. Regular firewalls and the way satellites are designed can't fix this issue (Cao et al., 2020, p. 202).

When data gets messed up or changed, either on purpose or by accident, it means someone is messing with the information while it's being sent or stored. This can cause problems with computer programs, hardware failures, using software without permission, or even someone intentionally changing the data to mess things up (Manulis et al., 2021). In space missions, if the instructions sent to a spacecraft get messed up, it can be really dangerous. If the spacecraft doesn't follow the right commands, something bad could happen. Using old or outdated software in a system is a known weak point. There's a list called Common Vulnerabilities and Exposures (CVE) that keeps track of known problems with this kind of software (Manulis et al., 2021). It's really important to keep software updated to fix these issues and avoid getting hacked. Ignoring updates can make the software an easy target for hackers.

Space doesn't belong to any one country. It's a global thing where there are no borders, which makes it tricky. Some people might secretly attack satellites floating up there, taking advantage of the lack of borders. This is a problem because it's hard to catch them in the act (Cao et al., 2020, page 202). The bad effects of these attacks are worse because it's tough to notice and follow these attacks on satellites. Sometimes, satellites break down not just because of attacks but also because of other problems like changes in space environment, mistakes in design, broken equipment, and defects (Cao et al., 2020, p. 203). It's challenging for ground stations on Earth to figure out what's happening up there because of the distance, weather, technical issues, and other things that hide the true story of the satellite, letting attackers get away with it.

As standard resource-limited systems, satellites suffer from computing and wireless resource limitations. Many satellites lack proper communication systems, making them vulnerable to attacks. Most satellites use basic transponders that don't unpack signals, making it hard to confirm data authenticity (Cao et al., 2020, p. 202). Attackers can exploit this weakness by sending penetrating signals to ground stations. They also use advanced systems to demodulate and extract data. This sneaky approach leads to stealing satellite information without permission. To complicate things, attackers use special codes to keep their communication secret, making it difficult to detect their actions. This underscores the importance of improving satellite infrastructure to prevent security risks and ensure the safety of satellite information (Cao et al., 2020, p. 202).

2.4.2 User segment

Satellite communication has a big issue called eavesdropping, especially for satellites in low Earth orbit (LEO), this problem can cause significant losses, so it's crucial to check and strengthen the system's security (Gerber, 2023, p. 56).

Bad actors use eavesdropping to act like real web users, posing a serious threat by sending harmful data to disrupt satellite systems (Manulis et al., 2021). The risk is higher with broadband internet via satellites due to the involvement of many users and devices (Gerber, 2023, p. 56). The problem gets worse because devices and satellites lack encryption, making it easier for attackers (Cao et al., 2020).

Cao et al. (2020) explain different ways that bad actors can mess with communication satellites. They discuss tricks like pretending a satellite card is a computer card, using old equipment for attacks, messing with low Earth orbit (LEO) satellites from other countries, and spying on data by moving satellites close together in a group (Cao et al., 2020). The geographical nuances of satellite orbits are exploited, with lower orbits facilitating network attacks akin to terrestrial pseudo-base stations for information interception (Cao et al., 2020, p. 201). For example, one particularly insidious method involves employing a torpedo attack akin to the 4G system, where the attacker uses legitimate ST to launch multiple paging operations on the targeted ST, thereby exposing user identification information. This exposed data can then be intercepted by LEO satellites and terrestrial equipment, allowing the attacker to track the user's location—a grave security threat (Cao et al., 2020, p. 202).

The proposed solution to this web of vulnerabilities is full-stream encryption for each link. However, many satellite internet providers find the associated overhead impractical compared to the benefits. In stark contrast, Starlink stands out by implementing hardware-based encryption on user link equipment, a robust measure to ensure user privacy and mitigate the risk of eavesdropping attacks (Starlink, 2023). In this way, Starlink demonstrates its commitment to advancing satellite technology and protecting user privacy and security in the evolving satellite communications environment.

2.4.3 Space segment

Once it enters the orbit, the satellite appears to have entered an area disconnected from direct human contact. But that doesn't mean it's completely safe. The computer programs and physical parts that control how a satellite works could be a target for problems. This makes the satellite vulnerable to attacks that could mess up its operations and security plans (Cao et al., 2020, p. 203). If a bad actor gets control of a satellite, they could even make it leave its planned path in space. This type of attack could go even further, with the intruder putting malicious codes into the satellite's system (Cao et al., 2020, p. 203). When the satellite comes back to normal operation, it could bring these issues with it. Basically, if hackers get hold of satellite technology, which was originally made to make satellites last longer, they could use it to take over satellites for their own purposes. According to Manulis et al. (2021), using certain technologies like software-defined radios (SDRs) and digital signal processing software can make these systems easy targets for hackers. This might lead to problems like service disruptions and network breakdowns. The study also shows that attackers could eavesdrop without creating a constant jamming signal. Despite having some defenses, SDRs still have weaknesses that require thorough testing to ensure they stay secure (Manulis et al., 2021).

The relationship between satellite and ground control systems and the effectiveness of security measures determine the likelihood of compliance. Altering a satellite's setup or path is tough. It takes a lot of skill and know-how to break into the systems that control it (called telemetry, tracking, and command networks) (Manulis et al., 2021). There's also a risk of more precise attacks using advanced methods like flexible software and playing back recorded messages. Even well-known companies and government agencies like NASA can be at risk, as there have been cases of satellites crashing due to external enemies messing with them (Manulis et al., 2021).

2.5 History of Starlink

In 2002, Elon Musk created SpaceX, an agency that has changed how scientists explore space. The company started with personal investments and grew into a top player in aerospace engineering. SpaceX made people enthusiastic about area exploration. They have notable achievements such as sending the first commercial shipment to the Space Station in 2012. SpaceX modified the rocket industry by way of making reusable rockets (Howell & Pultarova, 2023). This method they are able to use the identical rocket greater than once, saving a ton of cash on each release. Basically, SpaceX is the first private company to build a rocket that goes into space, launch a spaceship, make it orbit, and bring it back. They've also sent a spaceship to the International Space Station and transported astronauts there. It's like the use of a plane multiple instances rather than throwing it away after one flight. Starlink started out in 2014 when SpaceX applied for permission from Norway’s telecom regulator. However, the general public simplest discovered about it whilst SpaceX announced the launch of this new Internet provider. Elon Musk, the boss at SpaceX, played a crucial role in making Starlink better. In 2018, the government (FCC) said it was okay for SpaceX to start sending satellites into space. Starlink has two fundamental purposes for Musk and SpaceX. One is to provide high-pace Internet in underserved areas at a more reasonable price. The other purpose is to generate income to fund missions to Mars. The company got approval to installation over 7,000 satellites, with 4,000 approved in 2016. Military assessments began in 2018 to discern out how the satellites could be lanched. In February 2018, SpaceX efficiently launched its first Starlink test satellites named TinTinA and TinTinB (Howell & Pultarova, 2023).

2.6 Case studies on Satellite Internet

In a study by Shaengchart and Kraiwanit (2023), they talked about how satellite Internet, like Starlink, can really help people in faraway and rural places to grow their businesses. Shaengchart et al. (2023) further states that Starlink could change how people get the Internet, not just in big cities like Chicago, but everywhere. This change could be a big deal for things like education, health, and business, according to Shaengchart et al. (2023). A good and an ongoing example is from Nigeria where a team-up between Inmarsat and Instrat, a healthcare group, is trying to make healthcare better in places where there's no good land internet or reliable communication (Abdullah, 2022, p. 16). This program helped train healthcare workers through videos, making it easier to manage diseases. It showed real results, like successfully saving newborns and preserving women's lives during childbirth (Abdullah, 2022, p. 16). The collaboration also caused a big increase in reporting diseases, going from 20% to 65%. The speed and accuracy of analyzing data also got much better (Abdallah, 2022, p. 16). Basically, by combining satellite technology and working together, there's a big change happening. It goes beyond borders, helping communities around the world.

Starlink dreams of a future where satellite internet becomes super fast, reaching up to 1 Gbps when it's working at its best (Abdallah, 2022, p. 16). This big step forward in technology could change the way a society does e-health, not just through video doctor visits but also by making telesurgery possible. Imagine doctors in Europe using robots to do surgeries on people in faraway places in Africa (Abdallah, 2022, p. 16). At the same time, doctors will have better internet connections, making it easier to get patient information and offer medical help online (Shaengchart et al., 2023). Right now, this technology is complicated and expensive, but experts think it might get cheaper over time. That could mean having better internet in Africa, which could save lives. As fast internet becomes more common, students will be able to use online resources easily and attend virtual classes without problems. And for society in general, having fast internet for everyone can help close the gap between people who have access to information and entertainment and those who don't, like streaming services, especially in places where there aren't many other options.

The recent addition of SpaceX's advanced Starlink satellite system in Osaka's communication scene has caught the attention of many. Because Starlink satellites orbit close to Earth, people in the telecom industry in Osaka are thinking about how it could be useful (Shaengchart et al., 2023). Experts believe that Starlink could make Osaka's communication networks better and more reliable. They suggest improving internet services and offering high-speed internet to everyone (Shaengchart et al., 2023). Starlink might also help when there are problems with regular networks, providing a connection with fewer interruptions. However, some in the industry are worried that adding Starlink to Osaka's network might be tricky (Shaengchart et al., 2023). There's a chance it could cause issues and make the network not work as well. People are also concerned that Starlink might be too expensive for businesses and households in Osaka. This raises questions about whether everyone can afford to use it. Just like Shaengchart et al. (2023) states, we'll have to wait and see how Starlink impacts Osaka's telecommunication industry.

2.7 Regulatory requirements

For years, the Committee on National Security Systems (CNSS) has made careful guidelines to secure satellite communications in the national security mission area. One of these rule sets is CNSS Schedule 12, also known as CNSSP-12. This set of rules aims to build security into ground and space systems from the start of their design. It's not just about following rules; it shows a strong commitment to security. The rules suggest advanced techniques like authentication, encryption supported by the NSA for end-users, and using unpredictable bit streams. Together, these techniques create a strong shield, ensuring that any transmissions that seem predictable are systematically eliminated, guaranteeing confidentiality and integrity (Manulis et al., 2021). The CNSSP-12 rules mainly deal with how commercial satellites used for government work should be secure. But even other systems might officially get recognized as secure by following these rules. Many organizations that care about future security tend to stick to the CNSSP-12 process. Some companies are making their systems better on their own. For instance, the LeoSat group makes sure its data network is encrypted, similar to CNSSP-12. Meanwhile, Starlink stands out by having end-to-end encryption built into its system right from the start, making it a key feature.

3 METHODOLOGY

In this study, the used information was mainly from previous articles to learn about the security of satellite internet constellations. Mengist et al. (2020) emphasize that using existing literature is crucial for gathering information and exploring new areas. This paper opted for this approach to gain a deep understanding of the topic using reliable and scholarly sources. This paper's focus was on Starlink's security measures and potential threats. This paper used online sources like Google Scholar and research gate, as well as popular platforms like Space X and Starlink. There was also use of news blogs for matters relating to Starlink. Key terms like "Starlink," "Satellite Internet Security," and "starlink cyber security" guided the search. Each source was carefully examined for information on Starlink's security system, potential threats, and other important details. As Snyder (2019) notes, a good literature-based research requires clear criteria for analysis, with the main goal being to understand key ideas and connections in the topic. Throughout this literature review, the paper adhered to ethical standards, recognizing their utmost importance in research. Any information was correctly cited and the author recognized. The intention was to comprehensively investigate the security of satellite internet constellations, using a method that allows for a thorough understanding of the subject. Systematic reviews, crucial for influencing educational policies, require careful consideration of ethical aspects, as explained by Suri (2020, p. 50). Creating and using these reviews has significant ethical implications, emphasizing the need for accurate representation of authors' and participants' viewpoints from the original studies to avoid any oversights (Suri, 2020, p. 51). This careful approach highlights the importance of giving credit through proper attribution and citation, ensuring acknowledgment of the original authors' valuable contributions.

4 STARLINK’S OPERATION AND SECURITY

This chapter summarizes a detailed study about the security of Starlink. It looks at three main things: how Starlink operates, the problems and vulnerabilities in its security, and the measures it currently takes to stay secure. By combining all this information, people get a good understanding of how safe Starlink is right now. This knowledge forms the basis for future talks and suggestions.

4.1 How Starlink Works

As mentioned before, unlike the solitary geostationary sentinels positioned at 35,786 km, the Starlink group has thousands of satellites that are much closer, just 550 km above us. Figure 4 shows the difference in distance between a GEO and a Starlink satellite. This setup gives internet coverage worldwide, going beyond what traditional satellites can do. Because Starlink's satellites are so close, they make internet activities faster, with a delay of only 25 ms. This is a big improvement compared to the slow 600+ ms delay of other satellites far away. So, Starlink is changing how people use the internet, making things like streaming, online gaming, and video calls much smoother and quicker (Starlink, 2023).

SpaceX, the company behind Starlink, has successfully launched and brought back many satellites. Since 2018, they've completed at least 37 missions, putting Starlink satellites into space (Gerber, 2023, p. 50). By early January 2024, there are over 5,289 small satellites up there, communicating with ground stations. They plan to launch almost 12,000 more, and might even go up to 42,000. The Falcon 9 rocket, with reusable carbon components, powers these missions, keeping the satellites safe until they're in the right spot (Gerber, 2023, p. 50). Figure 3 displays the Falcon 9 Fairing with Starlink Satellites. In each mission, about 60 Starlink satellites are released, forming a group in the sky (Gerber, 2023, p. 50). It's like building a network of satellites to improve communication and internet access globally. Abdallah (2022) states that SpaceX's Falcon 9 and Falcon Heavy rockets are a game-changer, making space travel much cheaper with their innovative approach (p. 9). They're breaking free from the super expensive costs of sending satellite into orbit. The CEO of Spire Global, Peter Platzer, talked about this in an interview, pointing out how we've shifted from the government leading space projects to private companies leading the way. This isn't just about saving money; it could mean we're entering a new phase where there increased satellite production and technological advancements (Abdallah, 2022, p. 9).

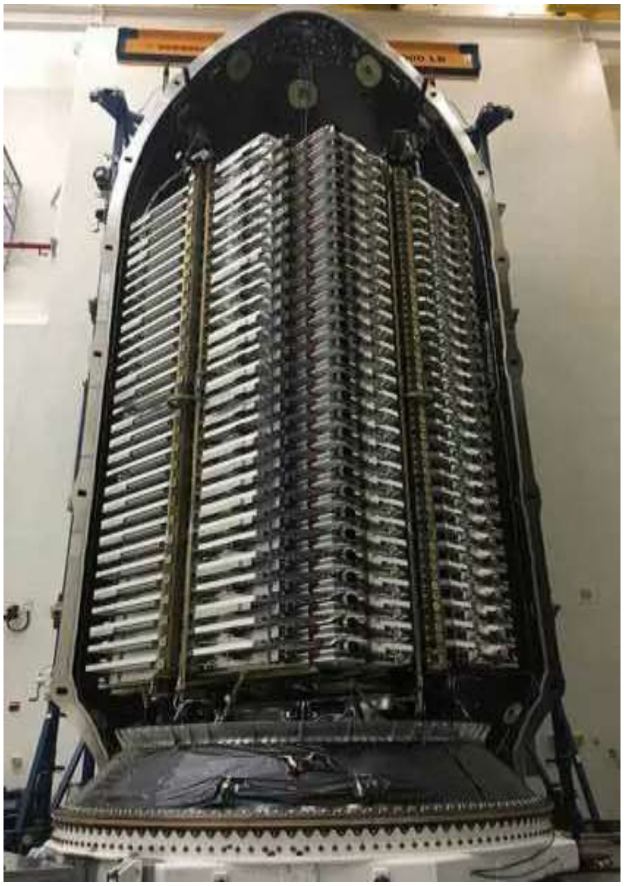


Figure 3: Falcon 9 Fairing with Starlink Satellites (Gerber, 2023).

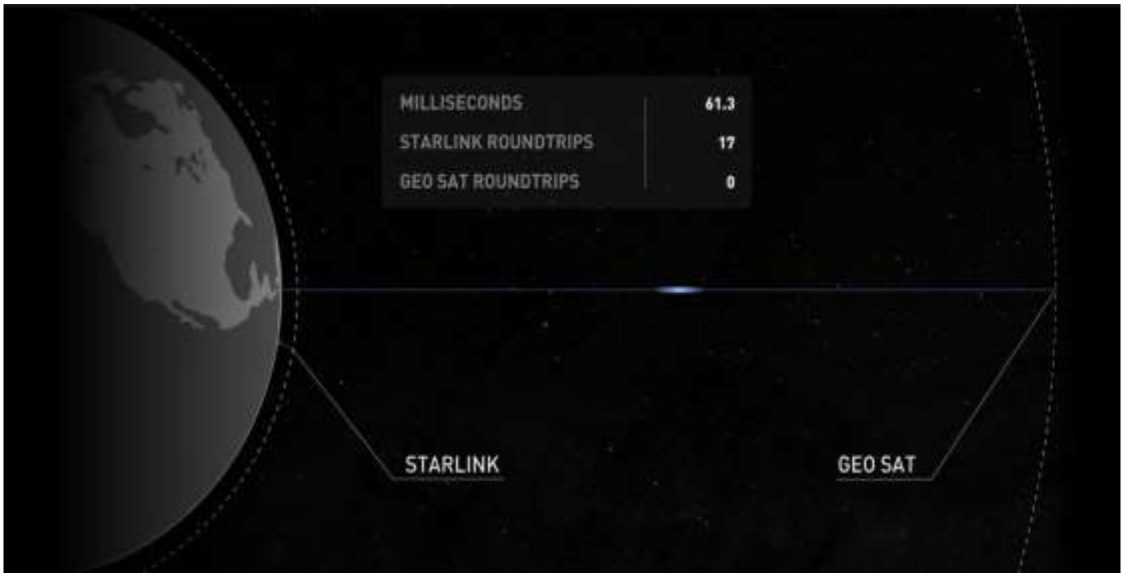


Figure 4: Starlink comparison to a GEO satellite (Starlink, 2023).

Starlink has many satellites in space, spread out in 72 paths, with about 20 satellites in each path. These satellites are designed to be simple, with one solar panel each, making everything easier (Starlink, 2023). The solar panels are all the same, which makes it easy to put them together. They work in a certain frequency range and weigh around 240 kg each (Herath, 2021). The satellites are flat and small, so they can be stacked efficiently for launching into space using SpaceX's Falcon 9 rocket.

Starlink's satellites are said to operate in autonomy when it comes to moving around in space (Starlink, 2023). They can avoid crashing into space debris or other satellites all on their own, which makes them super reliable and much safer than the usual standards in the industry (Starlink, 2023). These satellites have special sensors that look at the stars to figure out exactly where they are and how they're positioned in space. This helps them send high-speed internet signals in the best way possible (Starlink, 2023). And to travel through space, they use special engines that run on a gas called krypton, making Starlink one of the first-ever to use this innovative technology (Starlink, 2023). Starlink, uses advanced antennas for sending and receiving signals. They also use laser technology for communication between satellites (Starlink, 2023). Recently, they've started using optical space lasers on their satellites, which they call Optical Intersatellite Links (ISLs) (Starlink, 2023). This new technology allows them to transmit data globally without depending on local ground stations. In space, laser communication is 47% faster than traditional fiber networks on Earth (Herath, 2021). Starlink is always pushing the limits of technology. Each of their satellites has four strong antennas and two parabolic antennas, which make the network perform exceptionally well and handle more data (Starlink, 2023). This innovation is a big step forward in improving satellite communication.

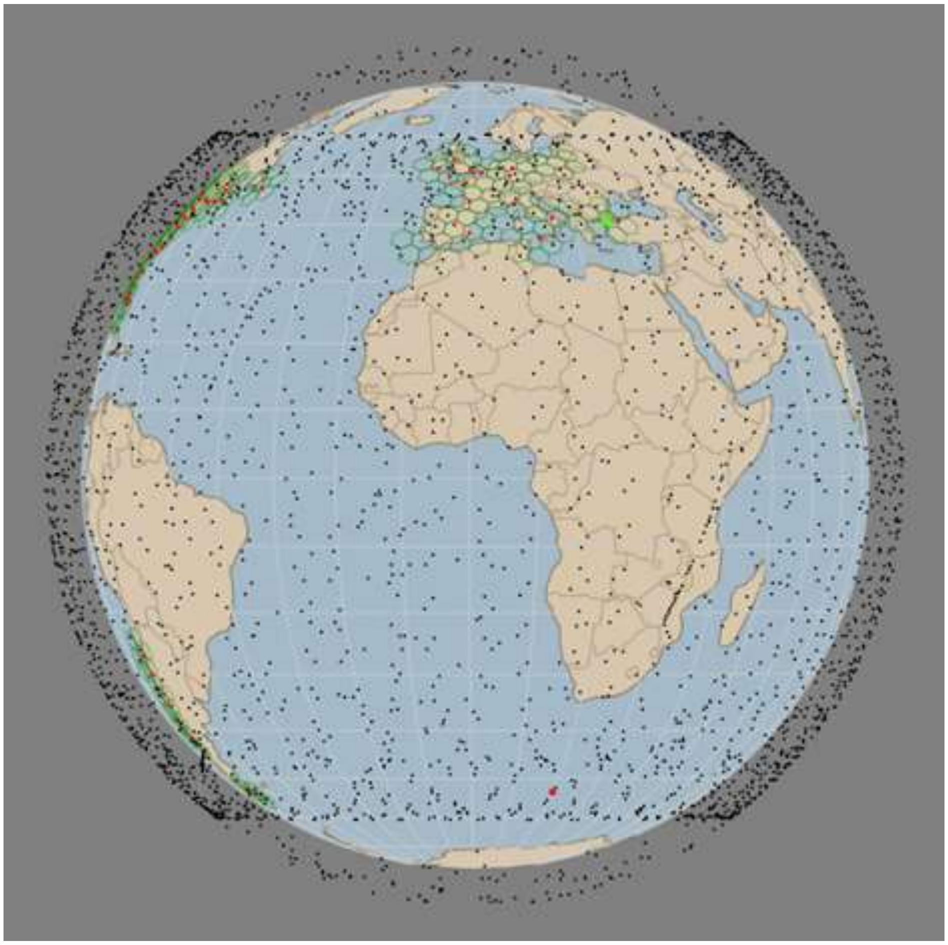


Figure 5: Starlink Satellite Map. Note. A black dot represents an individual satellite, with red showing a ground station (ITU & World Bank, 2023).

Starlink Gateways, also called Ground Stations, play a crucial role in keeping constant communication with satellites, enabling internet access and managing information flow to user terminals (Herath, 2021). Figure 5 showcases the placement of Starlink satellites in relation to Ground Stations SpaceX's satellite network uses the Ku band for communication with users and the Ku and Ka bands for communication between Ground Stations and satellites, making the system more effective (Herath, 2021). Since Starlink's satellites are placed closer to Earth, this results to creating small and precise beams. This closeness results in faster internet speed and lower delays, providing an impressive estimated total bandwidth throughput of 23.7 Tbps during the initial commercial deployment (Herath, 2021). The equipment for Starlink customers, officially called customer premises equipment (CPE), is easy to use, with a plug-and-play design that includes a satellite dish, Wi-Fi router, and power supply unit. The 23" diameter dish is manageable by one person and can be placed on the ground or rooftops with a clear view of the sky. Its self-orienting feature allows for quick connections, automatically aligning with Starlink satellites as long as there is an unobstructed view of the sky (Starlink, 2023). The dish's advanced technology, using a phased antenna array in a stacked honeycomb structure, ensures seamless alignment with orbiting Starlink satellites, making the system efficient and user-friendly. The Wi-Fi setup comes with a powerful router that connects well through a speedy Gigabit Ethernet port. It also supports Wi-Fi. Both the router and satellite dish use Power over Ethernet (PoE) for power. According to Herath (2021), one router can handle up to 128 devices simultaneously. The router operates on the IEEE 802.11 standard and functions at 2.4 GHz and 5 GHz, employing OFDM modulation technology (Herath, 2021). Starlink's commitment to cutting-edge technology ensures high-performance connectivity, playing a crucial role in addressing the global connectivity gap.

4.2 Security Issues and Weaknesses in Starlink

Starlink is working to give everyone around the world fast and reliable internet. They focus on making sure everyone gets fair access to the internet, balancing competition with public benefits, and keeping the system secure and reliable in this fast-changing field. But they are not perfect, this part of the paper will discuss the security issues in Starlink.

4.2.1 Cyber Threats and Issues

Starlink faces a major challenge regarding the potential involvement of malicious organizations. Cao et al. (2020) highlight a big worry for satellite internet providers: malicious actors may send harmful commands or inject viruses into satellite systems from Earth or space, trying to take control of the satellites (p. 197). This could lead to a loss of confidentiality, as these illegal groups may exploit low Earth orbit (LEO) satellites' observation capabilities to steal sensitive data from targeted countries (Cao et al., 2020, p. 196). Additionally, Yue et al. (2022) explain that LEO satellites, being closer to the ground, are more vulnerable to signal interference, and the wireless nature of their transmissions makes them easy targets for theft, risking privacy violations (p. 8). If a malicious actor manages to stay connected to Starlink's local network, they can control the system by sending commands from any device on that network (Smailes et al., 2023, p. 4). Even if they're subtle about it, they can still mess with the system's security. One sneaky way they might do this is through DNS hijacking. Here's how: when the device asks the network where "http://my.starlink.com" is, the attacker tricks it into going to their own server instead (Smailes et al., 2023, p. 4). Even if the client is using TLS (a security protocol), the browser isn't on high alert for a secure connection, leaving a vulnerability.

In the Russia-Ukraine conflict, Starlink satellites are helping Ukraine's military communicate. But using Starlink in Ukraine has risks because the equipment getting the signal can be located while in use. Elon Musk warned about this, saying Starlink is the only non-Russian communication system in some Ukrainian places, making it a potential target. He suggested users turn on the terminals only when needed and point the antenna away from crowded areas (Kolovos, 2022, p. 19). After the cyber-attack, SpaceX updated the software for Starlink terminals on moving vehicles to use less power and help the Ukrainian Armed Forces during power outages (Kolovos, 2022, p. 20). Unfortunately, these updated terminals were targeted, facing attacks that tried to access the mobile satellites without permission. Some terminals were successfully blocked initially, but a later software update allowed users to bypass these disruptions. In August 2023, during Ukraine's counteroffensive, a Five Eyes report revealed that Russian hackers had planted malware on Starlink, trying to steal data from Android tablets used by Ukrainian soldiers (Lyngaas, 2023). Ukrainian Security Services stopped some hacking attempts, acknowledging that Russian forces had captured tablets on the battlefield and loaded them with harmful software. According to Gerber (2023), when they investigated people who use Starlink for internet (the Starlink users) and compare them to those who don't use Starlink (the non-users), there's a noticeable link. Their data shows that Starlink users are experiencing more identity theft and damage to their reputation, which is a big worry.

4.2.2 Hardware Vulnerabilities and Misuse

According to Smailes et al. (2023), the Starlink router was once vulnerable to a cyber-attack that could disrupt its service by using tricky commands through its control system (p. 5). They fixed this problem, but it shows the challenge of balancing user-friendly design with keeping things secure. Making things easy for users sometimes makes it easier for attackers too. This was highlighted by an incident at a Black Hat security conference where a researcher named Lennert Wouters revealed vulnerabilities in Starlink's satellite security. Wouters used a simple $25 homemade mod chip to show how hackers could gain full control over Starlink's system and run their own code on its devices (Burgess, 2022).

Wouters, looking at it from a hacker's point of view, talked about how it's easier to hack into the Satellite through the user terminal instead of directly messing with the Satellite itself (Burgess, 2022). After finding these weaknesses, Wouters quickly told Starlink about them. Starlink, realizing how important this was, paid him through their bug bounty program. Even though SpaceX has made some updates to make it harder for these attacks, the main problem won't go away until they come up with a new version of the main chip (Burgess, 2022). This whole situation shows how cyber security is always changing, and Starlink need to stay alert and come up with new solutions to keep up with the risks.

People are worried that Starlink's satellites might be used to spy on others. Unlike regular cameras, satellites can see really big areas. According to Thummala's research in 2023 (p. 11), this kind of watching could help alert people about possible dangers, stopping bad things from happening. However, Lyons (2023) explains that Elon Musk's Starlink program is a big example of satellite spying (p. 11). Like Google Earth before it, Starlink is all about connecting people, and some say this focus helps overshadow concerns about potential misuse (Lyons, 2023, p. 12). Since Starlink aims to have thousands of satellites by 2035, it can be said they are providing real-time pictures for "persistent surveillance" (Kolovos, 2022, p. 28). While this might seem good for keeping an eye on things, it brings up a new worry: the chance of spying on people without them knowing or allowing it.

4.2.3 Regulatory Challenges

For Starlink to work well in any country, it needs official approval from the government to provide telecommunication services (Herath, 2021). Starlink's network is different because users can connect to the Internet without the direct control of their governments. While this gives users more power, governments might see it as a threat to their control (Herath, 2021). There's was no proof that Starlink has received this approval from any country in the global South (Herath, 2021). Starlink is in some African countries like Eswatini, Mozambique, Rwanda, Mauritius, Sierra Leone, Zambia, and Nigeria. In Zimbabwe and Botswana, officials are checking Starlink's request for a license to operate. To handle this issue, Starlink and governments need to work together to find a solution everyone can agree on. One idea is to set up at least one gateway in each country so that the Internet traffic goes through that point. However, local internet providers in these countries may resist this idea, seeing Starlink as a strong competitor (Herath, 2021). Also, the internet service in many global South countries is not great, so Starlink could offer better services, even in big cities where local providers are already operating. Dealing with this challenge requires everyone involved to work together to find a fair solution that benefits everyone, especially the users. Herath (2021) suggests using Starlink to improve the performance of local service providers by connecting their networks to designated gateways. This way, Starlink can positively contribute to the overall networking situation.

4.2.4 Physical Threats

While we often hear a lot about cyber security in the digital world, it's crucial not to overlook the importance of addressing physical security concerns. Imagine having multiple spacecraft in the lowest orbits (LEOs) – this creates a challenging situation for cooperative control. Factors like terrain adjustments, weather, and climate continually affect these spacecraft, making them deviate from their intended path (Yue et al., 2022, p. 15). In March 2021, a real-life incident involved the OneWeb satellite, which has a constellation of 35 satellites sent into space. There was tension because experts predicted potential clashes with the launch of Starlink satellites by the US military in September 2020 (Reed et al., 2021). To prevent a collision, OneWeb asked to turn off the automatic collision avoidance system on the Starlink satellite. Luckily, the satellites maneuvered around each other successfully (Reed et al., 2021). This event sparked debates, with OneWeb accusing Starlink of being careless about safety, while SpaceX (the company behind Starlink) played down the seriousness of the situation (Reed et al., 2021). It highlighted the tricky balance between advanced technology and responsible navigation in space, underscoring the potential damage to Starlink's reputation. So, even in this highly advanced technological world, managing the physical aspects of space security is a critical dance.

In a significant event, the United Nations Office for Outer Space Affairs shared that the China Space Station pulled off two clever maneuvers to avoid collisions in space. The first one happened on July 1, 2021, dodging a crash with the Starlink-1095 satellite, the second move occurred on October 21, 2021, steering clear of a potential clash with the Starlink-2305 satellite (Yue et al., 2022, p. 15).

These precise actions highlight the growing challenges of managing space traffic and potential dangers. As scientists explore space more, they're also creating a lot of space junk. This junk includes bits of spacecraft, tiny paint specks from space vehicles, rocket parts, and old satellites. The European Space Agency's stats, mentioned by Yue et al. (2022, p. 15), say there are about 1,036,500 debris objects bigger than 1 cm orbiting around. This space clutter zooms through space at over 28,968.12 kilometers per hour—way faster than bullets. It's a big danger to satellites in Low Earth Orbit (LEO) and puts them at risk of the scary Kessler phenomenon (Yue et al., 2022, p. 15). The LEO now has so much debris that it might cause a chain reaction of collisions, putting the future of space exploration in jeopardy (Yue et al., 2022, p. 15). The quick development and deployment of satellites using standard processes have shortened their lifecycles, increasing the chances of failure and potentially requiring replacement during use. This brings the realization of the Kessler system, which could further complicate space activities, closer to reality.

4.3 Starlink's Current Security Measures

After identifying the issues Starlink faces in regards to its security, it is also important to discuss the measures they have put in place to combat these issues. This section will discuss the measures put in place to protect clients.

4.3.1 Encryption and Authentication Protocols

Starlink takes data security seriously by using strong encryption and authentication methods for communication between client’s device and the satellites. Starlink also protects user data with advanced password management by LogMeOnce (2023), using 256-bit AES encryption to safeguard stored passwords. This makes it easier for users since they don't have to remember complex passwords. Researchers Zuo et al. (2023) recognized the security challenges in satellite communication and proposed a cutting-edge solution. They combined Advanced Encryption Standard (AES) with top-level channel coding, called super-encryption, to improve satellite network performance significantly (Zuo et al., 2023, p. 338). Starlink uses extra security steps like two-factor authentication and fancy biometrics (like fingerprints and facial recognition) to make sure only the right people can access their accounts (LogMeOnce, 2023). If the client’s password is weak, they warn the client to make it stronger. Verco (2021) says encrypting with AES on satellites is super effective (p. 93). With these security features, Starlink makes it hard for bad guys to sneak into their networks, keeping everything safe. Without a password, it's tough to stop bad websites or local users from messing with the administrator interface. Starlink's "guest mode" helps a bit (Smailes et al., 2023, p. 4). It lets users join a network without admin access, protecting against unwanted changes. It only let users access the admin interface on a special network that's not connected to the internet. That way, no one can mess with it from the outside. This stops any sneaky attacks from happening unnoticed.

4.3.2 Automation and Autonomy

At the forefront of Starlink's strong protection infrastructure lies a pivotal fusion of automation and autonomy within its satellite structures. The way satellites work is changing thanks to self-driving cars and advanced robots. Since the late 1980s, people have been working on making satellite operations more automatic and self-controlled on the ground (Manulis et al., 2021). This is all about satellites being able to do their thing without needing constant human control. This means the ground stations and control centers want to be able to tell satellites what to do without having to directly control every move (Manulis et al., 2021).

Saving money is not the only benefit; it also makes it easier to handle lots of satellites (Manulis et al., 2021). Trials using automatic ground stations and satellite operations prove this new approach is effective. Take SpaceX's Starlink satellites, for instance—they're built to track space debris and dodge crashes on their own (Manulis et al., 2021). This active control of their orbits doesn't damage the satellites; instead, it extends their lifespan and boosts their ability to withstand risks. This makes the Starlink system efficient overall, as shown by research (Manulis et al., 2021).

4.3.3 User Privacy

Starlink is actively safeguarding user data with strong measures in place to ensure privacy and security. Starlink takes privacy seriously, having a detailed policy on what information is collected, and how it's used, and protective measures. With strong technology, physical, and operational safeguards, they ensure personal data is safe from threats. Their well-designed approach assesses risks in processing tiny data bits (Starlink, 2023). Information sent via Starlink to client's device is encrypted for extra security. Starlink is careful about collecting data, only gathering what's needed for its service. This includes the client's name, contact information, payment details, and technical stuff like IP addresses (Starlink, 2023). They keep personal information as long as it's necessary, following the law's requirements. Usually, the client's account information stays for the account's life plus two more years, unless the law says otherwise (Starlink, 2023). Starlink is watchful for any possible data breaches. If they suspect a problem, they have strict steps to handle it. They inform users and regulators quickly.

4.3.4 User Education and Support

Starlink is all about keeping its users safe and informed. They don't just rely on technical stuff; they also teach and support users to be cyber smart. The main aim is to make sure people know the best ways to stay safe online. Starlink wants users to be active and strong in protecting their internet connections. In Africa, Starlink is doing cool things for space learning. They launched a program called Starlink for Education. This shows how serious they are about education and space stuff in Africa. According to Frąckiewicz (2023), Starlink gives free internet to schools and colleges in African countries like Nigeria, Kenya, Ghana, and South Africa. Starlink wants to give top-notch internet in Africa. This not only helps make money but also lets local communities join the world economy. Starlink is making a big impact in Africa by focusing on education, networking, and overall development (Frąckiewicz, 2023).

5 CONCLUSION

Starlink has emerged as a top contender when it comes to providing “internet from above.” As a result, people worry about possible weaknesses and security issues in its big, connected system. This research looked into how Starlink satellite internet service works, and identifying potential security issues and weaknesses in Starlink as well as evaluating how well Starlink’s current security measures protect against potential risks. Starlink Company has thousands of satellites that are much closer, just 550 km above us. This setup gives internet coverage worldwide, going beyond what traditional satellites can do. Because Starlink's satellites are so close, they make internet activities faster. Starlink also has some issues with its security as there have been instances of the system being hacked. Some examples include hacking by Russian hackers who planted malware on Starlink and Wouters who used a simple $25 homemade mod chip to show how hackers could gain full control over Starlink's system and run their own code on its devices. Factors like terrain adjustments, weather, and climate continually affect these spacecraft, making them deviate from their intended path. For Starlink to work well in any country, it needs official approval from the government to provide telecommunication services.

Starlink also has come up with measure to protect their systems and their clients from malicious actors. Starlink takes data security seriously by using strong encryption and authentication methods for communication between client’s device and the satellites. Starlink is careful about collecting data, only gathering what's needed for its service. Starlink is all about keeping its users safe and informed. They don't just rely on technical stuff; they also teach and support users to be cyber smart. Starlink is watchful for any possible data breaches. If they suspect a problem, they have strict steps to handle it. They inform users and regulators quickly. Based on the information in this study, Starlink is making sure its internet service stays safe and secure by always improving and keeping an eye out for problems. This is really important to make sure everything runs smoothly and people's information stays safe.

REFERENCES

Abdallah, L. 2022. Sustainability Impacts of Satellite Internet: Digital Inclusion vs. Environmental Sustainability.

Burgess, M. 2022. *The hacking of Starlink Terminals has begun*. WIRED UK. https://www.wired.co.uk/article/starlink-internet-dish-hack [Accessed 23 November 2023].

Cao, H., Wu, L., Chen, Y., Su, Y., Lei, Z., & Zhao, C. 2020. Analysis on the security of satellite internet. In *Cyber Security: 17th China Annual Conference, CNCERT 2020, Beijing, China, August 12, 2020, Revised Selected Papers 17* (pp. 193-205). Springer Singapore.

Coughlin, J. 2023. The Advancements and Future of Satellite Internet Technology. 10.13140/RG.2.2.30821.58081.

Deutschmann, J., Hielscher, K. S., & German, R. 2022. Broadband internet access via Satellite: Performance measurements with different operators and applications. In *Broadband Coverage in Germany; 16th ITG-Symposium* (pp. 1-7). VDE.

Frąckiewicz, M. 2023. *How does Starlink Handle Network Security and user privacy?* TS2 SPACE. https://ts2.space/en/how-does-starlink-handle-network-security-and-user-privacy/#gsc.tab=0 [Accessed 23 November 2023].

Gerber, C. J. 2023. *Cybersecurity Risk Effects of Starlink on Rural Populations in the United States* (Doctoral dissertation, Capitol Technology University).

Graydon, M., & Parks, L. 2020. 'Connecting the unconnected': a critical assessment of US satellite Internet services. *Media, Culture & Society*, *42*(2), 260-276.

Herath, H. M. V. R. 2021. Starlink: a solution to the digital connectivity divide in education in the global South. *arXiv preprint arXiv:2110.09225*.

Howell, E., & Pultarova, T. 2023. Starlink satellites: Everything you need to know about the controversial internet mega constellation. https://www.space.com/spacex-starlink-satellites.html#section-the-history-of-starlink [Accessed 23 November 2023].

ITU and World Bank. 2023. Digital Regulation Platform. https://digitalregulation.org/regulation-of-ngso-satellite-constellations/ [Accessed 23 November 2023].

Kolovos, A. 2022. Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict. *Air & Space Management and Control Laboratory*

Kvant, A., & Johansson, C. 2023. Secure satellite internet usage in high-risk areas. *Blekinge Institute of Technology*

LogMeOnce. 2023. *Starlink Password*. https://logmeonce.com/resources/2023/07/12/starlink-password/?__cf_chl_tk=yO1d7fOb8D971crgSkIGmlnGXVO3SPEhmjd2qY4H7Yc-1700069470-0-gaNycGzNDZA [Accessed 23 November 2023].

Lyngaas, S. 2023. *Russian military hackers take aim at Ukrainian soldiers' battle plans, US and allies say | CNN politics*. CNN. https://edition.cnn.com/2023/08/31/politics/military-hackers-russia-ukraine/index.html [Accessed 23 November 2023].

Lyons, S. 2023. Satellite surveillance and the orbital unconscious. *New Media & Society*, 14614448231187352.

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. 2021. Cyber security in new space: analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, *20*, 287-311.

Mengist, W., Soromessa, T., & Legese, G. 2020. Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX*, *7*, 100777.

Michel, F., Trevisan, M., Giordano, D., & Bonaventure, O. 2022. A first look at Starlink performance. In *Proceedings of the 22nd ACM Internet Measurement Conference* (pp. 130-136).

Reed, H., Dailey, N., Stilwell, R., & Weeden, B. 2021. Decentralized space information sharing is a key enabler of trust and the preservation of space. *Advanced Maui Optical and Space Surveillance Technologies Conference*

Shaengchart, Y., Kraiwanit, T., & Butcharoen, S. 2023. Factors influencing the effects of the Starlink Satellite Project on the internet service provider market in Thailand. *Technology in Society*, 102279.

Shaengchart, Y., & Kraiwanit, T. 2023. Starlink satellite project impact on the Internet provider service in emerging economies. *Research in Globalization*, *6*, 100132.

Smailes, J., Salkield, E., Birnbach, S., Strohmeier, M., & Martinovic, I. 2023. Dishing out DoS: How to Disable and Secure the Starlink User Terminal. *ArXiv preprint arXiv: 2303.00582*.

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339.

Starlink. 2023. *World's most advanced broadband satellite internet*. https://www.starlink.com/technology [Accessed 23 November 2023].

Suri, H. 2020. Ethical considerations of conducting systematic reviews in educational research. *Systematic reviews in educational research: Methodology, perspectives and application*, 41-54.

Thummala, R. 2023. Space Worms: On the Threat of Cyber-ASAT Weaponry to Satellite Constellations. *The Pennsylvania State University*

Verco, E. 2021. Satellites are cyber insecure: We need regulation to avoid a disaster. *ANU Journal of Law and Technology*, *2*(2), 57-94.

Yue, P., An, J., Zhang, J., Pan, G., Wang, S., Xiao, P., & Hanzo, L. 2022. On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends. *arXiv preprint arXiv:2201.03063*.

Zuo, P., Wei, J., Zhang, K., Liu, X., Guo, C., & Hu, R. 2023. An intelligent encryption decision method for autonomous domain of multilayer satellite network. *Alexandria Engineering Journal*, *81*, 337-346.