CYBERSECURITY RISK EFFECTS OF STARLINK ON RURAL POPULATIONS IN THE UNITED STATES

by

Christopher John Gerber

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Science in Cybersecurity

CAPITOL TECHNOLOGY UNIVERSITY

April 2023

CYBERSECURITY RISK EFFECTS OF STARLINK ON RURAL POPULATIONS IN THE UNITED STATES

Approved:

Mark Fearer, D.Sc., Chair

Timothy Robinson, D.Sc., Committee Member

Accepted and Signed:

Mark Fearer — April 21, 2023

Mark Fearer, D.Sc. — Date

Timothy Robinson — April 21, 2023

Timothy Robinson, D.Sc. — Date

Ian McAndrew — 21 April 2023

Ian McAndrew, PhD, FRAeS — Date
Dean, Doctoral Programs
Capitol Technology University

ABSTRACT

The general problem is the advent of low earth orbit (LEO) satellite internet changing the surface of internet-connected devices and users globally (Cao et al., 2020; Scanlan et al., 2019). The specific problem is the proliferation of Starlink LEO satellite internet access in the United States, which is changing the cybersecurity risk profile of rural American customers (Scanlan et al., 2019; Voelsen, 2021). A pre-test and post-test design was utilized with a quantitative, quasi-experimental approach to determine whether specific cybersecurity risk occurrences changed for those who purchased, installed, and used Starlink. The population of this study was rural participants in America who had pre-ordered but had not yet installed Starlink. The sample size was 49, and participants were taken from 22 states. Four research questions were proposed, each targeting specific Internet usage cybersecurity risks, including identity theft, data breaches, reputational harm, malware, and virus infection. A survey instrument was used to collect pre- and post-test data to analyze the treatment and control group participants. When comparing the treatment group (Starlink users) to the control group (those who did not use Starlink), the occurrence rate increased for identity theft and reputational harm, with a decrease observed for data breaches, malware, and viruses.

Keywords: cybersecurity, data breach, identity theft, malware, reputational harm, risk, satellite systems, SpaceX, Starlink, viruses

DEDICATION

I dedicate this dissertation to my family—my wife, Jamie, children, parents, and siblings. This research would not have been possible without my wife's unwavering dedication to our family. You have always encouraged me to maximize my life and potential; this feat is no exception. Dylan and Briella, although you may not remember the many hours this endeavor took away from us, I appreciate your good behavior toward your mother during this time. I hope this serves as inspiration for you to know that anything you set your mind to can be accomplished.

Mom and Dad, you made it your life's mission to provide for your children and encouraged me to accomplish anything, and I am forever grateful. Todd, thank you for always giving me a different perspective and knowledge. Most assume identical twins think and act alike; this is simply false! Jodi, your enthusiasm and thirst for life is infectious. Thank you for always keeping me honest. Bear, I could not have asked for a greater father-in-law and friend. I appreciate your continuous support.

ACKNOWLEDGMENT

First and foremost, I want to acknowledge my Chair, Dr. Mark Fearer. Sir, I appreciate your guidance, support, and tutelage throughout this process. I am genuinely grateful for your time reviewing, mentoring, and providing feedback. To my committee member, Dr. Timothy Robinson, thank you for your honest feedback and quantitative mindset. Your knowledge and review of my material gave me the data needed to make the relevant and appropriate changes required to achieve this goal.

To my fellow doctoral cohort members Charles, Conner, Devlin, Johnny, Kait, Kenya, Romeo, and Ronnie, I am grateful for your knowledge and the friendship we have gained while pursuing our goals together. You each brought a unique perspective and approach to the ever-changing field of cybersecurity, allowing me to grow truly.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Society can expect a "massive impact on the security and resilience of the global Internet" (Voelsen, 2021, p. 27) due to the advancements in low earth orbit (LEO) satellite technology. In the United States, the first to market in a large-scale deployment of this technology is Starlink, a subsidiary of SpaceX (Sheetz, 2021b). Elon Musk, the company's chief executive officer, stated during the *Satellite 2020* conference that the product will primarily serve rural areas with a low population density where competitors' technologies, such as 5G and other broadband products, are unavailable (Musk, 2020).

Scanlan et al. (2019) described internet access around the globe, especially in rural areas, as rapidly changing and stated that this shift inevitably changes the attack surface for devices and users previously not connected to the Internet. Specifically, the advent of LEO constellations to provide this access must be tracked "to analyze potential security concerns related to S.I." (Cao et al., 2020, p. 193). Companies will face several technical challenges during deployment, and the consequences of success will significantly impact their customers (Voelsen, 2021). This study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite Internet upon rural American customers.

Chapter 1 provides an introduction to LEO satellite internet and its cybersecurity-related effects on the primary Starlink customer base. It discusses the research problem, purpose, significance, and nature of the study. The framework, questions, limitations, delimitations, and critical definitions are also covered.

Background of the Study

The Internet is a single, interconnected, worldwide framework comprising commercial, administrative, instructive, and other computer systems and networks (Shirey, 2007). In 1969,

the United States government conceived the early version of the Internet—ARPAnet—which allowed disparate computer systems to communicate (National Science Foundation, 2003). In 1983, the widespread adoption of a standard for communication called the transmission control protocol/internet protocol (TCP/IP) started the Internet down a path of rapid growth (Ryan, 2010). Since then, connectivity to the Internet has been commercialized, resulting in numerous internet service providers (ISPs) (Rueter, 2019).

Takei and Murai (2003) described how the Union of Soviet Socialist Republics launched the first satellite in 1957 to provide a communication medium in geostationary (GEO) orbit. In 1975, the first satellite connection to use TCP/IP was completed in a joint effort by Stanford University, Raytheon, and the University College London (Takei & Murai, 2003). Until 1986, the Internet, including any satellite communication, was limited to academic institutions and government organizations. The National Science Foundation Network (NSFNET) was the first implementation to allow internet users to conform to a standard that permitted the quickest growth ever (National Science Foundation, 2003). The first company to have a commercial offering for satellite internet was Hughes in 1996 with the Viasat product (Hughes Corporate, 2021). It offered a download-only service with a modem dial-up for uploads. Since then, satellite internet speeds have increased to the Federal Communications Commission (FCC)-defined broadband level of 25Mbps, competitors have emerged, and bi-directional communication is considered standard (Daehnick et al., 2020).

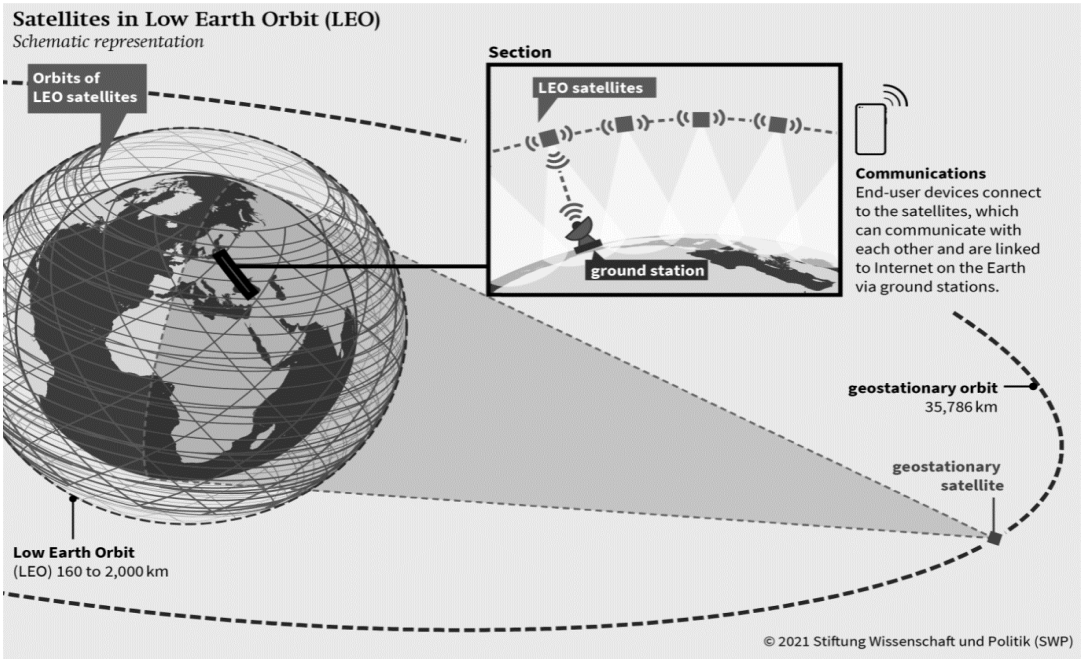
Non-LEO-based satellite internet faces a primary challenge with current technology—network latency (Berlocher, 2009). Gartner (2021a) described latency as the time taken for a packet of information to be transmitted between disparate nodes. Berlocher (2009) stated that although many advancements have been made to increase the speed of GEO Internet offerings,

the distance the satellites orbit the Earth is the primary reason latency is higher than terrestrial-based ISPs. For example, Miller (2017) stated that Viasat satellites operate approximately 22,300 miles from the Earth's surface, resulting in an average latency of 638 milliseconds (ms). In comparison, other terrestrial-based broadband providers potentially may provide a latency of less than 30 ms (Miller, 2017).

Voelsen (2021) described the fundamental difference between LEO and GEO satellites providing internet access as their distance from Earth; GEO operates at 35,786 km, while LEO operates at 160 to 2,000 km (Voelsen, 2021). Due to this distance and the Earth's rotation, GEO satellites appear stationary, whereas objects in LEO rotate the Earth 12-16 times every 24 hours, depending on the altitude (Borthomieu, 2014). Figure 1 represents this relative distance.

Figure 1

Orbital Distance

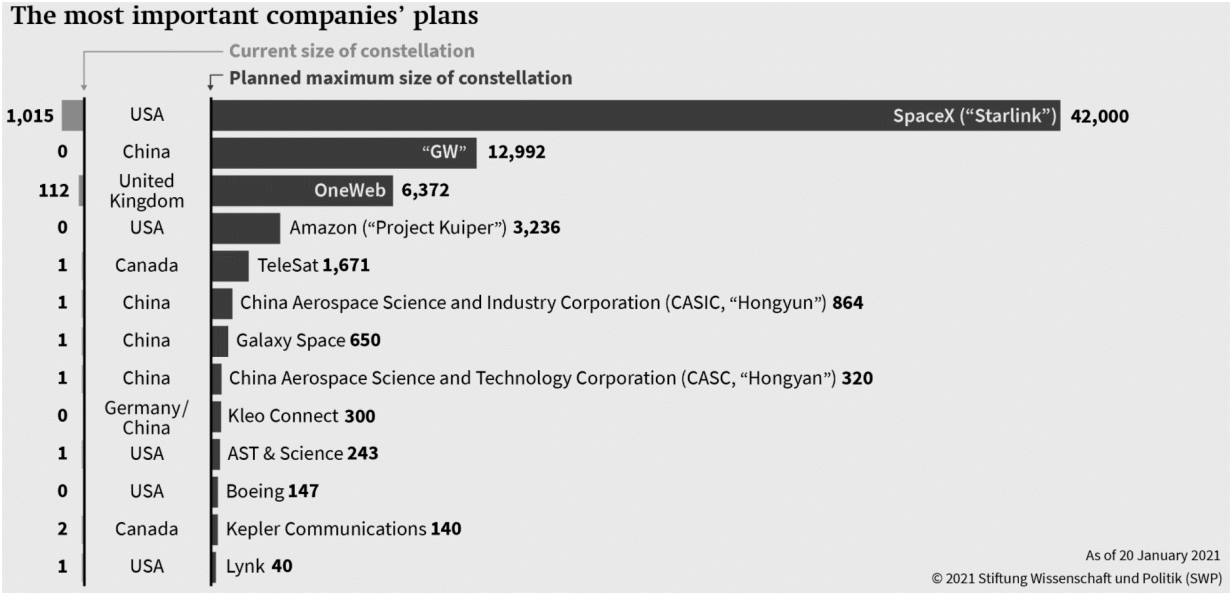


Note. From *Internet from space: How new satellite connections could affect global Internet governance,* by Voelsen, D., 2021, German Institute for International and Security Affairs. (https://doi.org/10.18449/2021RP03). Reprinted with permission.

Del Portillo et al. (2021) described that during the early 1990s, several companies submitted applications to offer telecommunications services from LEO; however, cost overruns and lack of funding were some factors that limited their success. After 20 years of technology improvements and cost reductions, numerous organizations have submitted new applications to the FCC for LEO satellite deployments to service the United States (Del Portillo et al., 2021). From a size and scope standpoint, the influential organizations are Amazon, OneWeb, SpaceX, and Telesat (Del Portillo et al., 2021). SpaceX's Starlink product was chosen for this study because of its deployment size and plans. More information on this choice is found in the importance section of this chapter. Figure 2 depicts the current and planned LEO constellation sizes as of January 2021.

Figure 2

LEO Satellite Internet Companies



Note. From *Internet from space: How new satellite connections could affect global Internet governance,* by Voelsen, D., 2021, German Institute for International and Security Affairs. (https://doi.org/10.18449/2021RP03). Reprinted with permission.

Although cyber risks exist on the Internet (Federal Bureau of Investigation, n.d.), this study focused on occurrence rates of identity theft, personal data breaches, reputational harm, malware, and viruses for the end-users of Starlink. The United States Department of Justice (2020) defines identity theft as the wrongful possession of a victim's data to be used for financial gain. In 2019, the United States saw $3.5 billion in losses reported due to this crime. (Federal Bureau of Investigation, 2019).

A personal data breach is when an "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" occurs (Information Commissioner's Office, n.d., p. 2). These breaches include intentional and accidental causes (Information Commissioner's Office, n.d.). In research from the North Carolina Department of Justice (2021), a record number of 1,644 personal data breaches were reported in the United States in 2020 by corporations, a 36% increase from the number recorded the previous year. Reputational harm is a negative shift in an individual's perception due to an outside source (Agrafiotis et al., 2018). Malware and viruses are software designed to cause harm to users, applications, or hardware (Zhong et al., 2022).

An insignificant amount of data related explicitly to the risk factors of Starlink technology on end-users was found in scholarly and peer-reviewed research, representing a possible gap in the literature that will be further examined in Chapter 2. This section covers the history and status of satellite Internet ISPs, LEO, and the cybersecurity risks of financial theft, data loss, reputational harm, malware, and viruses.

Problem Statement

The general problem is that the advent of low earth orbit satellite (LEO) Internet is changing the surface of Internet-connected devices and users globally (Cao et al., 2020; Scanlan et al., 2019). As stated in the background portion of this introduction, satellite Internet is not a novel concept. However, the LEO market has an estimated annual growth rate above seven percent (The Business Research Company, 2021). Starlink leads the way with over 1,000 satellites with plans to launch over 12,000 to provide Internet access anywhere (Posadzki, 2020). With this growth comes a lack of scholarly and peer-reviewed research into the possible effects of this technology. The specific problem is that the proliferation of Starlink LEO satellite Internet access in the United States will change the cybersecurity risk profile of rural American customers (Scanlan et al., 2019; Voelsen, 2021).

Purpose of the Study

The purpose of this study was to determine the cybersecurity risks posed by Starlink LEO satellite Internet upon rural American customers. Specifically, it focused on the incidence rates of identity theft, personal data breaches, reputational harm, malware, and viruses for the end-users of Starlink. This information was obtained using a pre- and post-test survey.

This study focused on data that does not exist, based on a gap in the current literature discussed in Chapter 2. A population is "the entirety of some group" (Salkind, 2018, p. 261). The basis of this study is the human population, specifically the rural population in the United States that has pre-ordered but not yet installed or utilized Starlink. The results of this study will help educate and present data in a clear, concise manner for consumption.

Significance of the Study

As of June 2021, Starlink had over 500,000 pre-orders for its service in the United States (Sheetz, 2021b). The FCC has "approved SpaceX to launch 11,943 satellites, with the company aiming to deploy 4,425 satellites in orbit by 2024" (Sheetz, 2021a, p. 1). In the United States alone, approximately 14.5 million people do not have adequate access to the Internet via a broadband connection (Federal Communications Commission, 2020b). With an average of 2.62 people per household (United States Census Bureau, 2020), the pre-orders in the United States will represent over 1.3 million people directly affected by this technology. This study is unique because it was conducted during the early stages of the product's rollout, allowing for a targeted population and using pre- and post-test design.

Preliminary research showed that a body of knowledge on this topic does not exist. Several studies on the vulnerabilities of each satellite technology segment were found and are described in the background section of this chapter. The end-users and organizations deploying LEO satellite internet must understand the possible cybersecurity effects on those utilizing the product. This study aimed to add to the technology and end-user aspect of Starlink to ensure that all stakeholders understand the cybersecurity risks associated with the use of Starlink.

Nature of the Study

Creswell and Guetterman (2019) expressed that quantitative studies are static and investigate relationships between factors. In contrast, qualitative studies involve developing questions to determine ideas and thoughts (Creswell & Guetterman, 2019). This study used an independent and dependent variable to examine if a cause-and-effect relationship exists.

Furthermore, pre-experimental, true-experimental, and quasi-experimental designs were examined to determine the most appropriate quantitative approach. Non-experimental approaches were not considered, as they are qualitative (Salkind, 2018).

Pre-experimental designs anticipate the problems that causal inference may pose, and pre-experiments are used as an exploration method to determine if further experimentation will be beneficial (Frey, 2018). In this study, the problem identified already has substantiating evidence indicating a need for further research. Therefore, a pre-experiment design was not considered necessary.

Salkind (2010) described true experimental designs as having a minimum of one dependent and one independent variable. The main characteristic of this design type is the randomization of the treatment placed upon what is being studied (Salkind, 2018). Although the present study has a dependent and an independent variable, this design's randomization was inappropriate. The dependent variable was the occurrence rates for each cybersecurity risk, while the independent variable was the installation and use of Starlink. Also, this study was targeted, meaning that only individuals who have pre-ordered Starlink but have not installed it were chosen as the study population.

Salkind (2018) described quasi-experimental designs as having a single but significant difference compared to pre-experimental and true-experiential designs. He stated that the "hypothesized cause of differences you might observe between groups has already occurred" (Salkind, 2018, p. 194). A fundamental assumption of the present study was that the assignment to groups had already occurred. Therefore, for this study, a quasi-experimental design was utilized.

This study surveyed rural Americans who had pre-ordered but had yet to install and use Starlink. The same customers from the pre-test survey were included in the post-test survey, and both surveys were multiple choice based on the research questions to determine if a change in cybersecurity risk has occurred. As previously discussed, a quantitative methodology was utilized in this study. This method was considered most appropriate because the cause and effect of using Starlink were to be determined. A pre- and post-test experiment was performed on a control group. Salkind (2018) described this as a four-step process:

1. Randomly assign the subjects to the experimental or control groups.
2. Pre-test each group on the dependent variable.
3. Apply the treatment to the experimental group (the control group does not receive the treatment).
4. Post-test both the experimental and control groups on the dependent variable (in another form or format, if necessary). (p. 185)

The main difference between the approach defined and the one used in this study is the treatment administration. In this study, the researcher did not have control over Starlink's purchase, installation, and use; therefore, the treatment was not randomized by the standard method—a table of random numbers (Saint-Germain, n.d.). The manufacturer and customer determined the treatment schedule based on a contractual agreement.

Hypotheses/Research Questions

This quantitative research study aimed to determine the relationship between the deployment of Starlink and the primary end-user cybersecurity risk. The four research questions for this study, along with their appropriate alternate and null hypotheses, are as follows**:**

RQ1. Will the occurrences of identity theft change for end-users of Starlink in rural locations in the United States?

H_a1: Identity theft occurrences observed will increase between the control group and those exposed to the treatment of Starlink.

H_01: Identity theft occurrences observed will not increase between the control group and those exposed to the treatment of Starlink.

RQ2. Will the occurrences of a personal data breach change for end-users of Starlink in rural locations in the United States?

H_a2: Personal data breach occurrences will increase between the control group and those exposed to the treatment of Starlink.

H_02: Personal data breach occurrences will not increase between the control group and those exposed to the treatment of Starlink.

RQ3. Will the occurrences of reputational harm change for end-users of Starlink in rural locations in the United States?

H_a3: Reputational harm occurrences will increase between the control group and those exposed to the treatment of Starlink.

H_03: Reputational harm occurrences observed will not increase between the control group and those exposed to the treatment of Starlink.

RQ4. Will the occurrences of malware and viruses change for end-users of Starlink in rural locations in the United States?

H_a1: Malware and virus occurrences observed will increase between the control group and those exposed to the treatment of Starlink.

H_01: Malware and virus occurrences observed will not increase between the control group and those exposed to the treatment of Starlink.

With quantitative research, it is essential to prove that a relationship exists between two or more variables (Salkind, 2018). To do this, a researcher must first prove the null hypothesis false. This process informs the researcher about whether the results are due to chance or manipulation of a phenomenon (Creswell, 2012).

Theoretical and Conceptual Frameworks

The worldview approach to this study was defined as that of a postpositivist. Creswell and Guetterman (2019) describe this philosophy as determining effects based on a cause and state that the issues explored by postpositivists reflect the necessity to identify and evaluate the factors that influence results, such as those discovered through experimentation (Creswell & Guetterman, 2019). This research determined whether a direct cause-and-effect relationship existed between using Starlink and security risks. This approach influences the framework as described below.

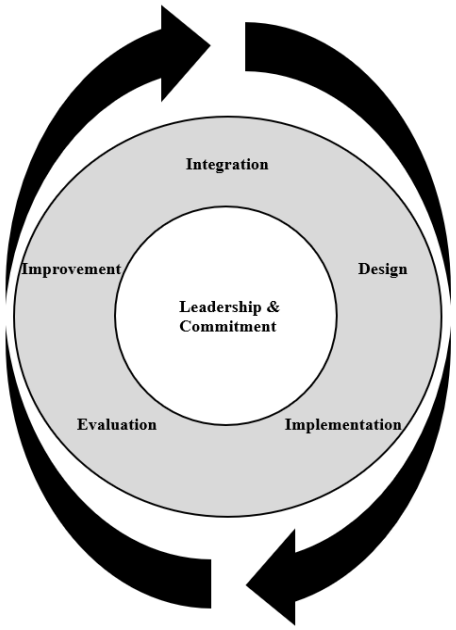
Grant and Osanloo (2014) described a theoretical framework as the basis for an entire dissertation. They stated that it is the foundation for constructing and supporting research and determines how best to approach a dissertation from a philosophical, epistemological, methodological, and analytical standpoint (Grant & Osanloo, 2014). Within the realm of cybersecurity, multiple frameworks to identify and mitigate risk exist, which was the main purpose of this study (Blake, 2021). For example, the Federal Information Security Management Act of 2022 is a United States Government framework designed to protect critical information and systems against threats (Cybersecurity & Infrastructure Security Agency, 2021). The National Institute of Standards and Technology (NIST) also developed the NIST Cybersecurity

Framework to perform a similar function (National Institute of Standards and Technology, 2021a).

This study used a theoretical risk management framework to inform and educate Starlink and associated end-users. Rather than attempting to modify a cybersecurity-specific framework to meet the needs of the study, ISO 31000 was used as a guide to assess the associated human risk. This standard provides management principles, processes, and definitions to identify and remediate risk (International Organization for Standardization, 2018). Figure 3 shows the framework at a high level. Central to the design is that the organization's leadership must be committed to risk management, ensuring it is built into all aspects of their business (International Organization for Standardization, 2018).

Figure 3

Theoretical Risk Framework



Note. Adapted from *ISO 31000*, by International Organization for Standardization, 2018 (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en). In the public domain.

The International Organization for Standardization (2018) lists five steps that must be performed continuously to identify and mitigate risk for all products. First, there must be an understanding of the individual or group goals. Second, the context of design must also be understood at length. Third, all stakeholders must be adequately educated on the product and understand all associated risks. Fourth, continuous evaluation of the product risks must occur regularly. Finally, any risks and framework identified must be monitored and adjusted continuously (International Organization for Standardization, 2018).

Conceptual frameworks are "indeterminist in nature and therefore do not enable us to predict an outcome" (Jabareen, 2009, p. 3). As previously discussed, the researcher chose the theoretical framework of ISO 30001 to meet risk identification needs. The choice of this method negated the use of a conceptual framework.

Definitions

The following terms are used throughout this paper. Defining them is essential to understanding this research.

- *Cybersecurity*. Various means of protecting computer systems from unauthorized usage (Seemmal et al., 2018).
- *Hacker*. Information system user who gains access unauthorizedly without authorization (National Institute of Standards and Technology, 2022).
- *Inclination*. The orbital angle of an object when compared to the equator of the Earth (Riebeek, 2009).
- *Internet Service Provider*. A business that provides its customers access to the Internet (Gartner, 2021b).

- *Internet*. The global network system containing academia, commercial, civic, and various entities that share a common technical standard (National Institute of Standards and Technology, 2021b).
- *Low earth orbit*. "Encompasses Earth-centered orbits with an altitude of 2,000 km (1,200 mi) or less" (Elburn, 2021, para. 1).
- *Network Latency*. The amount of time measured for a packet of information to be transmitted (Gartner, 2021a).
- *Orbit.* A curved path that one space object follows around another object due to gravity (The European Space Agency, 2020a).
- *Rural*. An area in the United States not designated as urban (United States Census Bureau, 2019).
- *Satellite Constellation*. A grouping of satellites that share common control, purpose, and function (International Astronomical Union, 2020).
- *Satellite*. An object or vehicle intended to orbit the earth or another celestial body" (Dunbar, 2017).
- *Sensitive Data*. Data in the United States Privacy Act section 552a not listed as criteria to be protected to aid the nation's defense or foreign policy (National Institute of Standards and Technology, 2021c). This includes information about United States citizens, such as their social security numbers and financial, medical, and criminal history (Department of Homeland Security, 2021).
- *Urban*. An area in the United States containing at least 50,000 people (United States Census Bureau, 2019).

Assumptions

Assumptions are taken for granted as part of a study (Simon & Goes, 2010). The primary assumption in this study was that Starlink will continue distributing its product in the United States. If the company had paused or slowed this rollout, it may have significantly affected this study's results. Another assumption was that the participants currently had access to the Internet but most likely not high-speed Internet. The FCC defines high-speed Internet as "25 megabits per second (Mbps) for downloads and 3 Mbps for uploads" (Federal Communications Commission, 2015, para. 2). It was also assumed that participants had the aptitude and knowledge to recognize if a cybersecurity event had occurred, based on the questionnaire. Examples were given to clarify each question to the researcher's ability. More detail on this is provided in Chapter 3.

Scope, Limitations, and Delimitations

The scope of the study was to identify whether Starlink's use caused changes to end-users' cybersecurity risk profiles. The extent of the study intended to include representation from all 50 of the United States. Multiple choice pre- and post-treatment surveys were the data collection methods used. The goal was to use the information obtained to inform end-users and SpaceX about the cybersecurity risks of the Starlink product. Because treatment administration was being controlled by an outside entity, a control group was expected to emerge. This study's target population was Americans living in rural areas who had pre-ordered Starlink but had not installed or used the product. This study used a judgmental sampling technique. According to Frey (2018), "the goal of judgment sampling is to deliberately select units (e.g., individual people, events, objects) that are best suited to enable researchers to address their research questions" (p. 1).

Creswell (2012) described limitations in quantitative research as issues that a researcher identifies. This study has several limitations. The dependent variable—cybersecurity risk—was difficult to gauge based purely on survey results. Also, human factors and influences, such as knowledge of the topic and willingness to disclose the information, had to be considered. In addition, the researcher relied on the pre-test participants completing the post-test survey six months later. Many issues may have arisen where the post-test may not have been completed, limiting the results.

Delimitations are the boundaries a researcher sets to ensure their study's goals are reasonably met (Theofanidis & Fountouki, 2019). This study targeted United States-based customers in rural areas. The survey was also limited to households, and no business customers were studied. This research only included those who planned to purchase and install Starlink, as identified in the pre-test survey.

Summary

Chapter 1 provided a background of this study, including a brief history of the Internet, satellite technology, LEO ISPs, and the possible cybersecurity risks. The general problem was identified as the fact that the advent of LEO satellite internet is changing the attack surface for Internet-connected devices and users globally (Cao et al., 2020; Scanlan et al., 2019). The specific problem was identified as the proliferation of Starlink LEO satellite internet access in the United States, changing rural American customers' cybersecurity risk profile (Scanlan et al., 2019; Voelsen, 2021). This study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite internet to rural American customers. The significance of this study was described as Starlink having over 500,000 pre-orders for its service in the United States as of June 2021 (Sheetz, 2021b). The FCC has "approved SpaceX to launch 11,943 satellites, with the

company aiming to deploy 4,425 satellites in orbit by 2024" (Sheetz, 2021a, p. 1). The nature of the study was identified to be quantitative. This method was chosen as the most appropriate because the study aimed to determine the cause and effect of using Starlink. A pretest-posttest design with a control group was used. Four research questions and their subsequent alternate and null hypotheses were provided. The theoretical framework was discussed, with a risk management approach based on ISO 31000. Essential definitions were provided in addition to this study's assumptions, limitations, and delimitations. The next chapter is a literature review that provides a thorough history of satellite technology, the Internet, and specific cybersecurity risks.

CHAPTER 2: LITERATURE REVIEW

This quantitative exploratory study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite Internet upon rural American customers. ISPs have provided customers with internet access using satellite technology since 1996 (Hughes Corporate, 2021). This chapter reviews the historical and current literature on satellite systems, the Internet, LEO segment threats, data breaches, identity theft, reputational harm, viruses, and malware. This data provide a foundation for this chapter.

Creswell (2012) defines a literature review as a summary of the peer-reviewed research that contributes to the history and current data for a study topic. In addition, the literature review categorizes information obtained into primary, secondary, and general sources to allow the reader to comprehend it (Salkind, 2018). This review is divided into four sections: methodology, title searches, historical overview, and current documentation.

Methodology

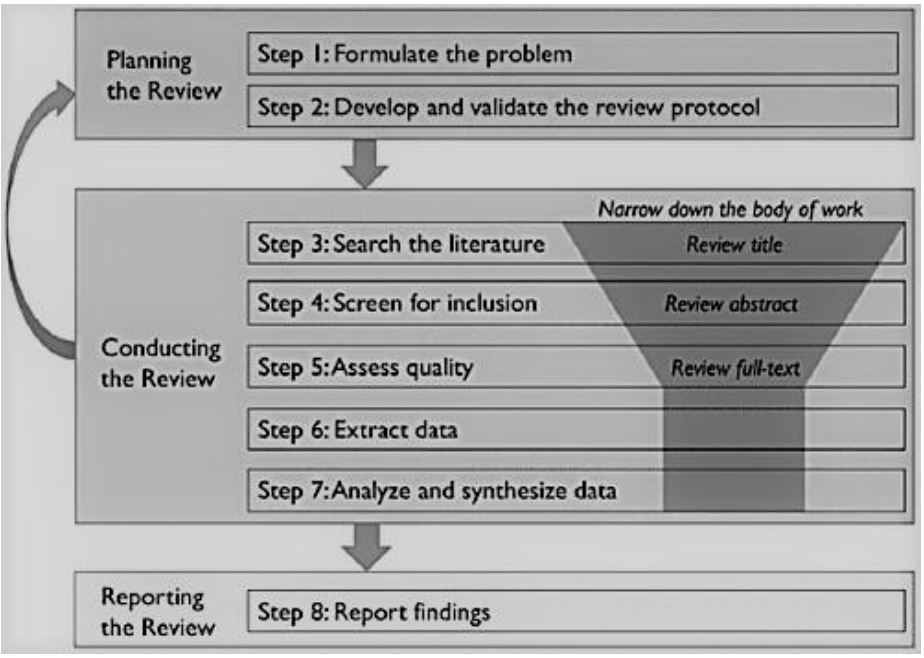
For this literature review, a systematic methodology was used. A systematic literature review (SLR) involves collecting and analyzing data systematically (Tikito & Souissi, 2019). According to the American Psychological Association (2020), peer-reviewed data is evaluated by professionals with appropriate qualifications before publication. In this chapter, as many peer-reviewed sources as possible were used for all sections except the current findings section.

An SLR involves eight steps (Figure 4): (1) problem formulation, (2) development and validation of the review protocol, (3) search of the existing literature, (4) filtering for inclusion, (5) quality assessment, (6) data extraction, (7) analysis and synthesis of data, and (8) report of findings (Yu & Watson, 2019). Additionally, an SLR is iterative, meaning it potentially may be

completed multiple times during the process (Yu & Watson, 2019). This process was used for subsequent collection and reporting in this chapter.

Figure 4

Process of Systematic Literature Review



Note. From Guidance on Conducting a Systematic Literature Review, by Yu, X., & Watson, M., 2019. *Journal of Planning Education and Research, 39*(1), 93-112. (http://dx.doi.org/10.1177/0739456X17723971). Reprinted with permission.

Problem formulation is the first step, based directly on this dissertation's research questions. According to Yu and Watson (2019), narrowing the problem to limit the amount of data to be reviewed is essential. Next is the review protocol, which specifies the details and protocol used. These protocols include the identification of the purpose, problem, inclusion and exclusion criteria, data extraction, and reporting procedures (Yu & Watson, 2019). Step three in the process is performing a literature search. It is vital to search quality library databases for peer-reviewed documents to use as sources of information (Yu & Watson, 2019). Step four is

screening for inclusion, where a researcher narrows the sources based on their ability to answer the research questions and specific problem statement (Yu & Watson, 2019). Next is quality assessment, wherein a deeper understanding of each source is obtained based on the full text (Ludvigsen et al., 2016).

Step six is data extraction, which, for qualitative studies, involves coding; however, for this dissertation, it involves the summarization of critical points (Yu & Watson, 2019). Step seven is the analysis and synthesis of data, where a more detailed analysis of sources is conducted to build on step six (Yu & Watson, 2019). The final step is reporting, where the process is shown visually to allow others to follow the steps and obtain the literature review data for themselves (Yu & Watson, 2019).

Title Searches, Articles, Research Documents, and Journals

This review focused on the peer-reviewed literature on satellite systems' space, user, and ground segments and their associated vulnerabilities. The tool used to conduct the review was the virtual library provided by Capitol Technology University. Several databases were used, including the Association for Computing Machinery Digital Library, EBSCOhost Databases and Services, Homeland Security Digital Library, IEEE Xplore, Nexis Uni, ProQuest Central, Puente Library Online Catalog, and Wiley Online - Decision Sciences. The inclusion criterion was data published between December 2016 and December 2021 from conference proceedings, books, professional journals, industry papers, and government publications. An exception was made while searching for data for the historical section, as satellite technology has existed for over 60 years and the Internet for 45 years. The keywords and phrases used to conduct this literature search included *satellite, satellite security, satellite ground segment, satellite user segment,*

satellite space segment, low earth orbit, satellite Internet, data breach, reputational harm, and identity theft.

The search yielded 241 sources, including peer-reviewed journals and government documents. The researcher then exclusively chose electronic documents and current website content due to the topic's recent history. Table 1 shows a summary of the search performed for this study.

Table 1

Search Detail Summary

Key Word(s) Used	Peer-Reviewed Journals	Government Documents	Books
Satellite	25	10	2
Satellite Security	15	7	1
Satellite Ground Segment	15	6	1
Satelitte User Segment	6	4	2
Satellite Space Segment	18	12	3
Low Earth Orbit	13	8	2
Satellite Internet	8	6	2
Data Breach	11	12	5
Reputational Harm	9	7	8
Identity Theft	12	8	3
Total Reviewed (241)	132	80	29

Each source was examined to form the historical overview and current findings sections below. Steps three through seven in the SLR were performed to narrow the data and body of work to extract only relevant content. Not all sources listed within this summary were included, as some content was deemed irrelevant to this study. The literature map used for Chapter 2 is shown in Appendix A.

Historical Overview

Satellite and Internet technology have evolved from their conceptual beginnings to the advanced technological innovations of today. To track the history, this portion of the literature review focused on the 1940s to 2010. It is separated into decades, each with an individual focus and shift leading to a significant change in each field.

Satellite Technology: 1940s

Sir Arthur C. Clarke envisioned early satellite communications after his publication in *Wireless World* in 1945 titled "Extra-terrestrial relays" (Evans et al., 2011). Clarke proposed that three satellites be placed in synchronous orbit to allow communications anywhere. Based on gravitational pull and speed, Clarke detailed what is now known as GEO orbit, some 22,230 miles from the surface of Earth (Pelton, 2010). Many perceived his predictions as fiction, including the editor who relegated his work to the middle of the publication. In 1945, the transistor had yet to be invented. Using the existing technology of vacuum tubes proved problematic, with Clarke estimating that a full-time crew needed to replace them (Pelton, 2010). The United States Army also had a classified study called *Preliminary Design of an Experimental World-Circling Spaceship* in 1946 that showed how synchronous communications satellites were used with similar technology. However, it had little impact on a global scale (Evans et al., 2011). Clarke's early visions have become a reality, with thousands of satellites performing the exact function he had envisaged (Evans et al., 2011).

In 1947, the transistor was invented by John Bardeen, William Shockley, and Walter Brattain while employed at AT&T's Bell Labs (Pelton, 2010). This technological advancement replaced the vacuum tube, eventually allowing electronics to operate in space with minimal failures (Brinkman et al., 1997). Over the next few years, modifications culminated in a licensed

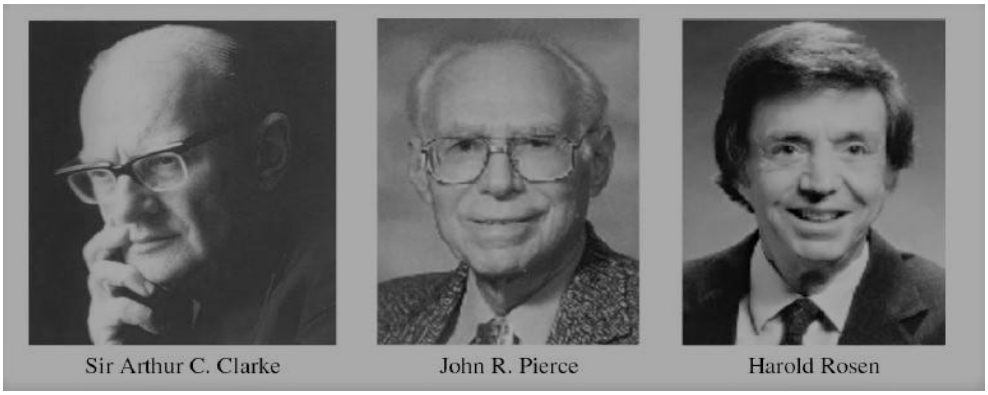
technology that was mass-produced and incorporated into electronic devices (Brinkman et al., 1997).

Satellite Technology: 1950s

The realization and implementation of the early visions of the 1940s characterized the next ten years of satellite technology. In 1954, another AT&T Bell Labs employee, John Pierce, envisioned satellites transmitting a radio signal over long distances between ground stations. However, Pierce saw no conceivable reason to replace land-based systems such as microwaves or cabling with satellites (Evans et al., 2011). Pierce was also the first to propose medium orbit constellations with potentially lower latency but requiring more satellites than GEO orbits (Evans et al., 2011). In addition to AT&T, many United States companies, including Lockheed-Martin, Hughes Aircraft, and RCA, began investigating satellite technology to expand their operations (Evans et al., 2011). Figure 5 shows the early pioneers within the satellite industry.

Figure 5

Early Satellite Pioneers



Note. From 65 years of satellite history from early visions to latest missions, by Evans, B., Thompson, P., Corazza, G., Vanelli-Coralli, A., & Candreva, E., 2011. *Proceedings of the IEEE*, *99*(11), 1840–1857. (https://doi.org/10.1109/jproc.2011.2159467)

Reprinted with permission.

Unknown to the United States, the Union of Soviet Socialist Republics (USSR) government had been rapidly developing satellite technology and the rockets needed to launch them into orbit throughout the early 1950s (Newell, 2010). On October 4, 1957, the world changed drastically with the successful launch and orbit of the first artificial satellite—Sputnik (Siddiqi, 2000). Before the launch, the USSR had announced plans to place a satellite into orbit during the General Assembly of the International Union of Radio Science in Boulder, Colorado (Swenson, 1997). Due to a large amount of USSR propaganda during this time, it was dismissed by many in the scientific world as fictitious (Swenson, 1997). Proving them wrong, Sputnik was launched and transmitted a simple radio signal back to Earth on the 40Mhz frequency for one month before becoming inoperable (Swenson, 1997).

Joseph Stalin's death in 1953 was a turning point for the USSR, with Nikita Sergeyevich Khrushchev emerging as an influential figure (Siddiqi, 2000). Khrushchev's lack of familiarity with the defense industry and the inner workings of the rocket and space program allowed for a "great degree of flux and ambiguity in the chain of command in the missile programs during the four-year period from 1953 to the first Sputnik launch in 1957" (Siddiqi, 2000, p. 119). This period of rapid growth allowed the USSR to outpace the United States in the satellite field.

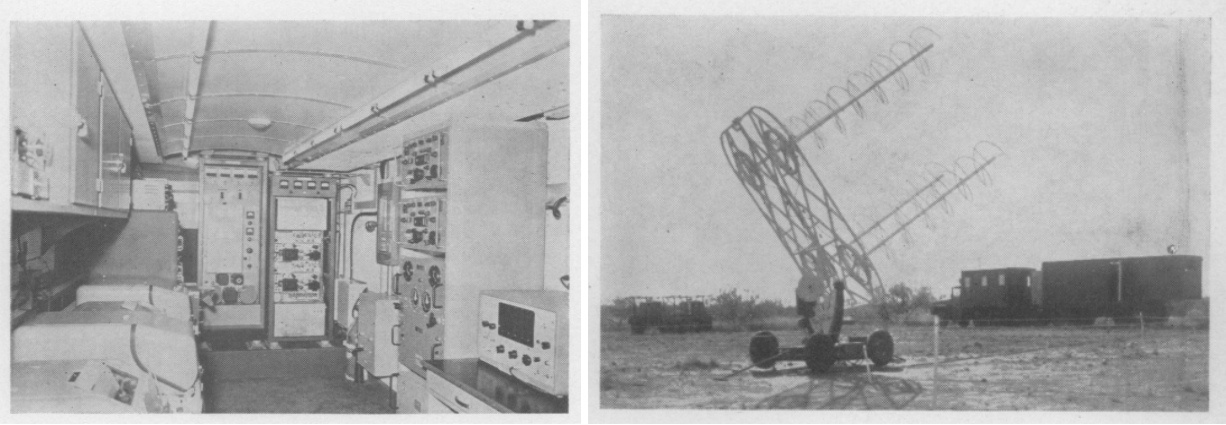
The United States entered the satellite industry with the successful launch of Explorer 1 on January 31, 1958. A joint venture by the United States Army Ballistic Missile Agency, the Jet Propulsion Laboratory, and the University of Iowa, Explorer 1 orbited Earth until March 31, 1958, making its final radio transmission on May 23, 1958 (Evans et al., 2011). After the launch, the United States moved quickly to create the National Aeronautics and Space Administration (NASA) by passing the Space Act on July 29, 1958, with an official opening on October 1, 1958. The objectives of the law, according to NASA (2008), are to:

- enhance the knowledge of space and the atmosphere;
- create and improve vehicles to operate in space;
- develop space vehicles to transport living organisms and related equipment into space;
- conduct scientific studies in space for long-term benefits to humans;
- ensure that the United States emerges as a leader in the field of technology in space;
- create a central location to make data available for the enhancement of United States interests, including military and non-military agencies; and
- improve the United States' cooperation with allies to preserve peace through space.

The United States launched the first telecommunications satellite—Signal Communications by Orbiting Relay Equipment (SCORE)—in December 1958. Its purpose was to prove that a signal was able to be transmitted from Earth to a satellite in space and back in a relay fashion (Brown, 1960). It proved successful, transmitting 14,000 words from ground stations to the satellite and back, with the most famous being President Eisenhower's Christmas holiday message to the American people (Brown, 1960). SCORE was only operational for 12 days but proved extremely valuable to future satellite telecommunication systems (Brown & Senn, 1960). SCORE included a ground station and antenna for transmission and tracking. Figure 6 shows these components.

Figure 6

SCORE Ground Equipment



Note. From Project SCORE*,* by Brown, S., & Senn, G, 1960. *Proceedings of the IRE*, *48*(4), 624–630. (https://doi.org/10.1109/jrproc.1960.287438)

Reprinted with permission.

Satellite Technology: 1960s

The 1960s showed rapid expansion of satellite technology, with an increase in the number of satellites and organizations involved in the industry. In a 1960 speech, United States President Eisenhower presented a view of the future of satellites as follows:

> The commercial application of communications satellites, hopefully within the next few years, will bring all the nations of the world closer together in peaceful relationships as a product of this nation's program of space applications. This nation has traditionally followed a policy of conducting international telephone, telegraph, and other communications services through private enterprise, subject to government licensing and regulation. I have directed the National Aeronautical and Space Administration (NASA) to take the lead within the Executive Branch both to advance the needed research and development and to encourage private industry to apply its resources toward the earliest

> practical application of space technology for commercial civil communications requirements. (Pelton, 2010, p. 25)

This statement and subsequent actions by NASA set the stage for rapid advancement from non-government organizations, including those in telecommunications and aviation (Pelton, 2010).

The Communications Satellite Act of 1962 established an international system open to countries. The International Telecommunications Satellite Organization (Intelsat) was formed due to this act, with 84 countries participating, each with a unique entity created for this purpose (United States Accountability Office, 2004). Slotten (2015) mentioned that to accomplish the goals listed in the Communications Satellite Act of 1962, the United States created a private company called Comsat which served to organize and execute the following goals:

- Serve the communications needs of the United States and other countries without discrimination.
- Provide global coverage.
- Encourage maximum private company participation.

The bill also outlined the responsibilities of NASA, the FCC, and the President of the United States (Slotten, 2015). NASA's role was advisory, providing technical expertise where applicable (Slotten, 2015). The FCC's role was to ensure competition and a zero-tolerance policy for discrimination. The President was to act in a supervisory role, overseeing the operations and development of satellite technology (United States Government Publishing Office, 2022).

Militaries also recognized the communication advantages satellites brought to the battlefield. In 1966, the Initial Defense Communication Satellite Program was created in the United States; it launched 28 satellites into GEO orbit over ten years for the Department of Defense. These were eventually used for surveillance during the Vietnam War (Evans et al.,

2011). The United States and the United Kingdom also agreed in 1966 to jointly develop and launch satellites for military use through a program called Skynet (Evans et al., 2011). The unique needs of the military led to numerous advancements in satellite technology and are discussed in more detail in subsequent sections of this chapter.

Satellite Technology: 1970s

The 1970s were a period of rapid growth for satellite communication, with many of the groundbreaking advancements of that time still in use today. These advancements include the Global Positioning Service (GPS), internet transmission over satellite links, and satellite imagery to map changes to the Earth's surface (Bonnor, 2012; Takei & Murai, 2003). This decade also saw a dramatic uptick in the use of these systems by the military (Bonnor, 2012).

In 1972, the United States Navy launched a satellite called *Timation* capable of precise timekeeping (Bonnor, 2012). Although this innovation was critical to calculating the position of ground objects, it was limited because it only provided two dimensions. Shortly after, the United States Air Force began researching a three-dimensional system called Project 621B (Bonnor, 2012). Bonnor (2012) also mentioned that in 1973, the United States Deputy Secretary of Defense merged the two projects—*Timation* and Project 621B—into the Navstar GPS. GPS is still in use today, with many advancements leading to its implementation in navigation systems such as smartphone applications; it is also used for pinpoint accuracy during military operations (Sturdevant, 2014).

The University of Hawaii was the first to use satellite technology in 1974 to connect to what will eventually become the Internet (Seymour & Shaheen, 2011). The Aloha project started as a simple radio network for transmitting data from one location to another, as the University had campuses in disparate sites (Abramson, 1985). The ATS-2 satellite connected the Aloha

network to other universities and government sites, including NASA's Ames Research Center in California, the University of Alaska, and Tohoku University in Japan (Abramson, 1985). The satellite link operated at a maximum speed of 56 Kbps using a single voice channel, according to Abramson (1985).

Another significant advancement during this decade was the first use of satellite imagery. In 1972, the first Earth Resources Technology Satellite was launched by NASA to record the Earth's surface (National Research Council, 2013). Later renamed Landsat, the program provided a stream of previously unseen images. Subsequent launches in 1975 and 1978 provided the continuity we enjoy today, with continuous operation for over 49 years (National Research Council, 2013). The program provides critical data on changes to land due to urbanization, weather events, and climate change and is used extensively in research (United States Geological Survey, 2019).

Satellite Technology: 1980s

The 1980s was a decade of increased satellite usage and dependency, especially in communications capabilities. The decade also saw significantly more countries launching satellites into orbit (Evans et al., 2011). Television broadcasting via satellite links was also launched during this decade (Takei & Murai, 2003).

Although initially deployed in the late 1970s along with the Marisat program, satellites used for mobile communications expanded to include commercial and military use throughout the 1980s. The United States Navy's Fleet Satellite Communications System became operational in 1981 and provided ship-to-land and land-to-ship communication (McGlade, 2010). Marisat's usage continued to expand, with significant ship carriers using it until retirement in the late 1990s (Pelton, 2010). Additional satellites also included packages for maritime use, such as

systems from INTELSAT and Experimental Communications satellites operated by the European Space Agency (Pelton, 2010).

From the time of its inception up until 1980, only twelve countries had successfully launched and operated satellites in orbit. These countries included The United States, the Soviet Union, the United Kingdom, Canada, Italy, France, West Germany, Japan, China, the Netherlands, India, and Czechoslovakia. During the 1980s, three more countries—Mexico, Israel, and Bulgaria—and the European Space Agency, a multi-country conglomerate, joined this list (Evans et al., 2011; Pelton, 2010).

In 1981, a small company—United States Satellite Broadcasting—was formed to deliver satellite television services to customers (Takei & Murai, 2003). They offered customers premium channels such as HBO, MTV, and Cinemax using analog signaling, traditionally serviced from coaxial-based services. In 1989, the Motion Picture Expert Group released a set of standards for digital television (Takei & Murai, 2003). This event allowed for a rapid expansion of cable television and led to the formation of companies like DirecTV.

Satellite Technology: 1990s

The 1990s saw continued innovation and increased funding and participation in satellite technology. For example, the Hubble, the first satellite to feature a telescope, was launched by NASA in 1990 (Webb, 2015). Similarly, the first satellite constellation for GPS was completed in 1993 (Bonnor, 2012). Although not ready for consumers, expanding the K_a frequency for satellites in 1993 opened the door for satellite internet offerings (Yen, 2002).

The ability of satellites to view long distances changed dramatically in 1977 when NASA embedded a telescope in a satellite (Webb, 2015). Originally called the Large Space Telescope, it was renamed Hubble in 1983. Testing was completed in 1985, but the NASA space shuttle

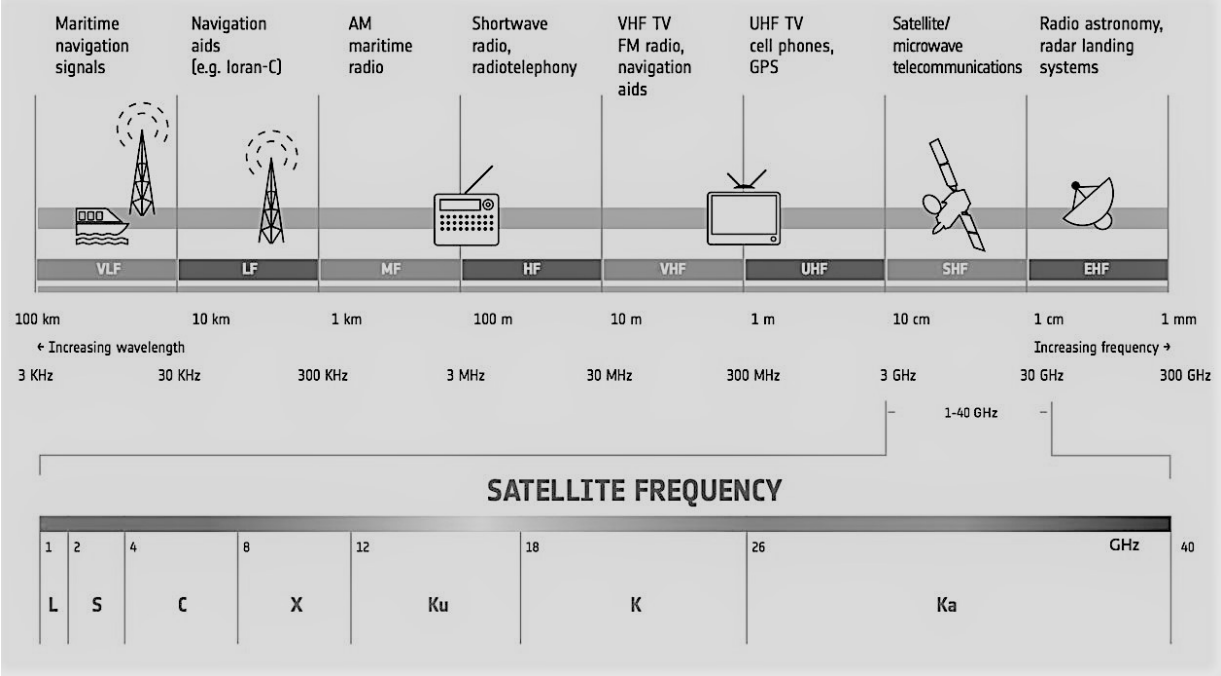
Challenger explosion in 1986 caused a delay until 1990 when Hubble was placed in the space shuttle Discovery and launched successfully into LEO (Webb, 2015). Hubble's contributions in this decade include determining a more accurate universe age in 1993 and confirming the existence of black holes in distant galaxies in 1994 (Garner, 2018).

In December 1993, GPS reached a milestone, with 24 satellites designated operational for civilian use in a constellation in medium-Earth orbit (Bonnor, 2012). After this announcement, the European Council passed a resolution specifying how the European Global Navigation Overlay Service will augment GPS to provide the accuracy needed for safety systems and other critical applications (Bonnor, 2012). Upgrades to software and ground stations continued to improve accuracy until July 1995, when the system was deemed fully operational (Bonnor, 2012). After this point, GPS began to take over traditional location services, which previously utilized ground-based radio signals (Cooper, 2019).

Satellites operate within seven frequencies (L, S, C, X, K_u, K, and K_a), offering increased wavelength and bandwidth at each level, with L being the smallest (Rogers et al., 1997). Figure 7 details each of these frequencies, along with typical applications. Until the early part of the decade, the use of the K_a frequency in satellites was limited, with government and military applications being the most frequent users. With the development and launch of the Advanced Communications Technology Satellite (ACTS) in 1993, NASA focused on K_a. ACTS significantly impacted the future of satellite communications (Rogers et al., 1997). "It is the first to have sophisticated telephone-system-type switching onboard. It can carry data at standard fiber-optic data rates with the same transmission quality, added performance, and cost savings that a land-based network provides" (NASA, 2002, p. 2).

Figure 7

Satellite Operating Frequencies



Note. From *Satellite frequency bands,* by The European Space Agency (2022). (https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands)

Reprinted with permission.

Satellite Technology: 2000s

The 2000s recorded several satellite changes, including increased privatization and technological innovations (Evans et al., 2011). The first consumer satellite high-speed Internet access in GEO was launched in 2004. In addition, investigation and testing began for satellites to operate in LEO to provide low-latency Internet access.

Intelsat, the intergovernmental consortium formed in 1964, became a private company in 2001 (Evans et al., 2011). This event was directly correlated to the passing of an amendment to the previously discussed Communications Satellite Act of 1962 in 2000. The amendment, titled

the Open Market Reorganization for the Betterment of International Telecommunications (ORBIT) Act, promoted a diverse and competitive global market for satellites (United States Accountability Office, 2004). The United States Accountability Office (2004) argued that although Intelsat's goal to become a private entity was realized, the amendment was not the driving force. Global trade agreements, trends, and improvements to market access during the 1990s were factors in the privatization.

In 2004, the successful launch of a GEO satellite named Anik F2 by the Canadian company Telesat showed that consumers were able to utilize the K_a band to gain enhanced throughput (Doan et al., 2004). Boeing Satellite Systems built it for multi-use and was "equipped with 24 C-band, 32 Ku-band, and 38 Ka-band transponders" (Doan et al., 2004, p. 1). Due to its size and antenna diversity, Telesat leased portions of the satellite to other companies. For example, United States companies like Viasat and Wildblue partnered with Telesat to offer high-speed Internet, using Anik F2 as the space component (Weiss, 2004). Anik F2 is still in service today, with many other satellites using the K_a band based on the success of this project. The next section will focus on the Internet.

Internet Technology: 1970s

The 1970s was a decade that saw the excessive growth of interconnecting disparate networks. In addition, numerous standards, including Transmission Control Protocol, Internet Protocol, and Ethernet, were created to form what eventually became the Internet (Campbell-Kelly & Garcia-Swartz, 2013).

The Internet is a collection of networks that share a common standard. These networks include academia, commercial, civic, and various entities (National Institute of Standards and Technology, 2021b). Early networks, including those at universities, banks, and government

sites, were implemented before 1970 but were unable to communicate due to a lack of standard protocols (Campbell-Kelly & Garcia-Swartz, 2013). For example, American Airlines had a private network running an application named SABRE that handled their global reservation service in 1961 (Campbell-Kelly & Garcia-Swartz, 2013). The Defense Advanced Research Projects Agency (DARPA) also had a network called ARPANET, created in 1965, that allowed select United States universities to participate. It was not until a universal standard was created that these networks communicated.

In 1973, two DARPA researchers, Vint Cerf, and Bob Kahn, began researching ways to improve radio network communications (Campbell-Kelly & Garcia-Swartz, 2013). Their work, titled *Request for Comments (RFC) 675, Specification of Internet Transmission Control Program*, was published in 1974 (Vinton et al., 1974). RFC 675 detailed the technology needed to deploy a packet-switching network beyond a private network through purpose-built devices called gateways. These gateways allowed the networks to talk to each other through a standard method (Vinton et al., 1974). The Internet is based on this RFC's standard named TCP/IP. TCP handles data broken into small packets by the source and reassembled by the destination, and IP ensures that each destination is accurate (Campbell-Kelly & Garcia-Swartz, 2013).

Another critical standard created during this timeframe was Ethernet. This technology allows two devices to communicate over a local area network (LAN). It was created by Bob Metcalfe, an employee at Xerox, in 1973 (Spurgeon, 2000). In 1976, David Boggs and Bob Metcalfe published *Ethernet: Distributed Packet Switching for Local Computer Networks* (Spurgeon, 2000). This article, published in the *Communications of the Association for Computing Machinery* journal, provided detail on packet switching, addressing, and reliability

built upon the TCP/IP standard created three years earlier (Metcalfe & Boggs, 1976). Together, TCP/IP and Ethernet created the building blocks for what we know now as the Internet.

Connectivity to the Internet throughout the 1970s was slow compared to the 1980s and 1990s. By the decade's end, over a hundred hosts were connected to the Internet via DARPA's backbone (Campbell-Kelly & Garcia-Swartz, 2013). Most of the users of the Internet were universities. The operation of DARPA's network was limited to those with United States Government grants. Because of this exclusivity, other institutions started distributed networks to share data. In 1977, Bell Laboratories created Unix-to-Unix Copy to share files and execute applications remotely (Campbell-Kelly & Garcia-Swartz, 2013). By 1979, it was used at over eighty sites, including many universities. It used its dial-up service, rather than the DARPA backbone, to connect each site.

Internet Technology: 1980s

With the basics of connectivity established, the 1980s were defined by steady growth and refining standards and protocols for internet use (Cohen-Almagor, 2011). This growth included the Domain Name System (DNS) and Internet Protocol version 4 (IPv4). It also saw the birth of commercial ISPs and focused on developing systems that utilized the Internet, such as the World Wide Web (Campbell-Kelly & Garcia-Swartz, 2013). It also marked the first time a widespread malicious attack occurred against internet-connected devices (Smith, 2015).

Ethernet, first created in 1973, continually evolved in this decade. In 1980, the need for standardization of LAN technology became apparent. In addition to Ethernet, other technologies such as Token Ring, Token Bus, and Carrier-sense multiple access with collision detection were created (Spurgeon, 2000). The Institute of Electrical and Electronics Engineers (IEEE), a United States-based standards organization, launched the *802 Project* to consider these technologies and

agree on a standard (Spurgeon, 2000). In 1983, IEEE approved the first standard for Ethernet called 802.3.

After 802.3, TCP/IP also evolved with the release of RFCs 791 and 793 in 1981. They represented the ninth edition of the standard initially published in 1974. These RFCs clarified technical controls and mechanisms to enhance the protocols (University of Southern California, 1981b). Although minor changes continued to be effected throughout the 1980s, these two standards are considered the definitive standards for TCP/IP today (Evans et al., 2011). RFC 791 also detailed an enhanced address schema with a numerical representation of Internet hosts, commonly known as IPv4 (University of Southern California, 1981a). This RFC was the fourth and final standard published for internet protocol.

Campbell-Kelly and Garcia-Swartz (2013) mentioned that internet hosts grew significantly after ARPANET moved to the RFC TCP/IP standards in 1983. Barely a year later, in 1984, the number of hosts nearly doubled from 562 to 1024 (Campbell-Kelly & Garcia-Swartz, 2013). At the time, a centralized file called HOSTS.TXT was maintained at Stanford University, containing a list of internet hosts' names and associated IP addresses. This file was updated anytime a new host joined and then downloaded by ARPANET sites for use (Pope et al., 2012). Constant updates to the file caused many problems, including name duplication and increased traffic load, resulting in its unavailability (Pope et al., 2012). To solve these issues, Paul Mockapetris, a researcher at the Information Sciences Institute of the University of Southern California, published RFCs 882 and 883 in 1983; these RFCs detailed the architecture for a system called the DNS (Pope et al., 2012).

Mockapetris (1983) described DNS as a distributed database. In addition to redundant core systems that hold copies of data, each internet site maintains its server, with other servers

performing lookups of the data they control. It performs a similar function to the HOSTS.TXT system but is more efficient and less error-prone (Mockapetris, 1983). IP addresses are translated to domain names using DNS (Mockapetris, 1983). For example, instead of remembering 198.185.159.145, a user will enter the domain name of www.weezer.com, making it more straightforward to interact with the Internet.

In 1988, the first instance of a widespread malicious attack against hosts connected to the Internet occurred (Smith, 2015). Named the Morris worm after its creator Robert Morris, a student at Cornell University, it was intended to map the known Internet at the time; however, its exploits caused many hosts to crash and affected 10% of Internet devices worldwide. The worm targeted vulnerabilities in the UNIX operating system and rapidly replicated on other hosts. It caused what is now known as a Denial-of-Service (DoS) attack. The United States government charged Morris with Computer Fraud and Abuse Act violations. In 1989, Morris was found guilty and received a financial penalty, community service, and probation (Federal Bureau of Investigation, 2018). This event forced administrators of networks to find ways to protect their internet hosts from malicious activity.

In 1989, the first commercial ISP was formed, offering fee-based services to the public. It was called *The World*, and its services were tied to telephone systems in the United States and Australia (Ryan, 2010). Before this, access to the Internet was limited to sites that DARPA and a few other organizations had authorized. This event led to massive growth over the next decade for other ISPs, allowing customers global access anywhere a phone line was placed (Ryan, 2010).

Furthermore, in 1989, a researcher in Geneva, Switzerland, named Tim Berners-Lee, presented an idea allowing internet users to browse documents and other file types via a standard

protocol (Cohen-Almagor, 2011). Berners-Lee named the system the World Wide Web. He also proposed and wrote the first internet browser that ran on the NeXTSTEP operating system and detailed the Hypertext Transfer Protocol, allowing a presentation and data transfer method when using a browser (Cohen-Almagor, 2011).

Internet Technology: 1990s

The 1990s was a period of rapid growth for the Internet. The number of clients, ISPs, applications, and commercial Internet participation grew significantly. With this growth came an increase in malicious activity and threats to users. It also saw the dissolution of the ARPANET Project and a boom in personal computers used in homes to connect (Cohen-Almagor, 2011).

Cohen-Almagor (2011) found that by the end of the 1980s, internet hosts totaled 159,000. By the end of the 1990s, that number had risen to 248,000,000, indicating a 155,875% increase. The decentralization of the Internet was a significant catalyst in this growth (Cohen-Almagor, 2011). In 1990, the ARPANET project was officially decommissioned (Meinel & Sack, 2014), and the National Science Foundation (NSF) had taken a more prominent role in previous years by introducing the NSFNET project, which provided connectivity for government entities and universities (Meinel & Sack, 2014). Responsibility for the remaining ARPANET sites was transferred to the NSF, marking the end of the project that started the Internet (Cohen-Almagor, 2011). Vinton Cerf, who co-authored the RFC in 1973 that led to the standardization of TCP/IP, famously stated:

> It was the first, and being first, was best, but now we lay it down to ever rest. Now pause with me a moment, shed some tears. For auld lang syne, for love, for years and years of faithful service, duty done, I weep. Lay down thy packet, now, O friend, and sleep. (Abbate, 2000, p. 195)

In 1991, three disparate ISPs came together in a mutual agreement called the Commercial Internet Exchange (CIX) (Campbell-Kelly & Garcia-Swartz, 2013). CIX allowed the ISPs PSINet, UUNET, and CERFnet to communicate, limiting the need for the NSFNET. Within a few short years, dozens of global ISPs joined CIX, leaving the NSFNET with limited connectivity responsibilities for everyday internet users (Campbell-Kelly & Garcia-Swartz, 2013). The United States remained the central hub for the Internet at the time, and it was not until 1994 that other countries, such as the UK, started to form their connectivity to the CIX (Campbell-Kelly & Garcia-Swartz, 2013). This connectivity led to the creation of internet exchanges globally.

Cohen-Almagor (2011) felt that the Internet was disconnected and difficult to navigate at the beginning of the decade. Applications developed for operation on the Internet, such as electronic mail clients and browsers, were non-intuitive for users (Dainow, 2017). Additionally, many applications relied on the non-graphical user interface (GUI) UNIX operating system to function. Operating systems such as Microsoft Windows and Mac OS brought the GUI into the hands of users and changed interoperability and use (Dainow, 2017). With the introduction of GUIs, many applications transformed into user-friendly offerings. Nowhere was this more prevalent than in the Internet browser (Cohen-Almagor, 2011).

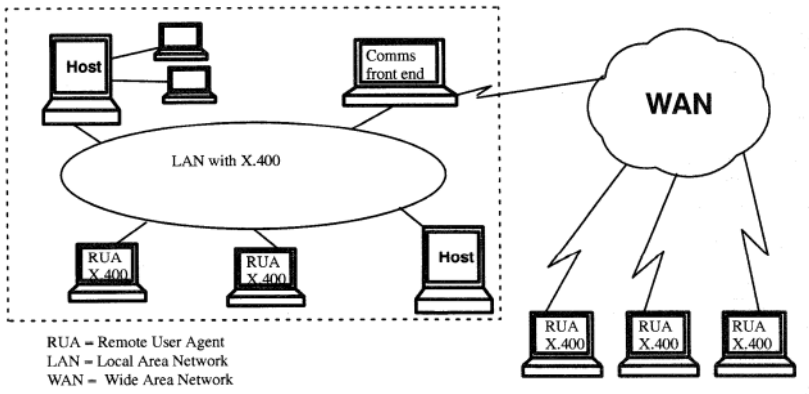
In 1992, only a few websites existed, with estimates of fewer than 30 worldwide (Campbell-Kelly & Garcia-Swartz, 2013). By 1993, 130 unique internet browsers existed, although most were experimental and text-driven. The MOSIAC browser was launched with a GUI-based point-and-click design. Because of its intuitive and user-friendly approach, it was downloaded over a million times and quickly became the browser of choice (Campbell-Kelly & Garcia-Swartz, 2013; Pope et al., 2012). According to Pope et al. (2012), the release of the

Netscape browser in 1994 and Internet Explorer in 1995 made the World Wide Web even more accessible. By the decade's end, websites totaled 50 million (Cohen-Almagor, 2011).

In addition to the World Wide Web and these websites, electronic mail, commonly known as email, went from relative obscurity to commonplace in ten years. Campbell-Kelly and Garcia-Swartz (2013) state that before 1990, less than three percent of personal computers globally used email. The lack of a standard protocol and interoperability between email systems were the leading causes of this lack of adoption. X.400, an email protocol first published in 1984 and updated in 1988, became the de facto standard in the early 1990s, and by 1995, it was used for email communication (Rotzal, 2002). Rotzal (2002) explains that X.400 is built so that any internet user potentially may message any connected person. X.400 is a similar system to the current postal service, with a from and to address in the form of a username and domain name. Figure 8 shows the high-level architecture of the X.400 standard.

Figure 8

X.400 Architecture



Note. From X.400 message handling system: the remote user agent, by Rotzal, P., 2022. [Paper Presentation]. Milcom '95, San Diego, CA, United States. (https://doi.org/10.1109/MILCOM.1995.483504). Reprinted with permission.

As more applications and users utilized the Internet as a communication system, malicious activity and threats to the users and their data were seen. As mentioned, the Morris worm in 1988 proved that the Internet was viable for conducting nefarious acts (Smith, 2015). The 1990s are described by Smith (2015) as the decade of viruses. The Melissa virus was the most notable in 1999 (Garber, 1999). The Melissa virus was propagated through email attachments with users' address books as the mechanism (Garber, 1999). Users were encouraged to open the attachment, which contained executable code that sent the same message to the first 50 users in the address book of the victims (Garber, 1999). The virus was meant to cause a DoS in email servers, and it worked. Disruption was rampant, causing an estimated $561 million for organizations to remediate (Garber, 1999).

Internet Technology: 2000s

The 2000s saw unprecedented global internet use for personal, business, and governmental growth (Cohen-Almagor, 2011). Moreover, ISPs utilizing satellite technology continued to evolve at an increased speed and with diversity (Takei & Murai, 2003). The 2000s also recorded increased internet threats, with more advanced malware, viruses, and data theft (Middleton, 2017).

In 2000, the Pew Research Center began tracking internet usage among United States citizens and found that by 2000, 52% of American adults had used the Internet (Perrin & Duggan, 2015). By 2010, the number had grown to 72%, representing a 24% rise over a decade. The reasons for this sharp rise in internet use were reportedly website access and email usage (Perrin & Duggan, 2015). According to Cohen-Almagor (2011), internet users totaled 361 million in 2000, and websites were at 50 million. By 2010, 1.9 billion people were internet users, with 2.69 billion websites.

Conducting business on the Internet grew alongside the increase in users throughout the 2000s. Wigand (1997) described this practice as electronic commerce. He stated that, "the bandwidth of electronic commerce spans from electronic markets to electronic hierarchies and incorporates electronically supported entrepreneurial networks and cooperative arrangements" (Wigand, 1997, p. 2). Shortened to the term e-commerce, global transactions conducted in this manner in 1999 were worth $150 billion (Terzi, 2011). By 2010, this number had grown to $572 billion, a 281% increase (Terzi, 2011). Most e-commerce transactions in the early decade (80%) were between businesses (Terzi, 2011). Consumer websites such as Amazon.com already existed and grew considerably over this period. According to Amazon, Inc. (2022), its total sales at the end of 2000 were $2.76 billion. Ten years later (in 2010), this figure grew to $34.2 billion, representing a growth of 1,139%. In 2000, customer item assortment was limited to books, music, DVDs, and videos. By 2010, products were available in almost every category imaginable, including Amazon Web Services cloud infrastructure (Amazon, Inc., 2022).

Governments worldwide also continued or started to use the Internet to conduct operations (Gilroy & Kruger, 2007). In addition to practical uses such as tax collection and information storage, many governments increased regulations and laws on the Internet (Gilroy & Kruger, 2007). As the Internet grew in size and content, censorship of the data contained therein also did. By 2009, over sixty countries had filtered content for their citizens (Koumartzis & Veglis, 2011). Although the United States was not one of these countries, many government efforts were passed to regulate or expand the Internet as an industry (Gilroy & Kruger, 2007). In 2005, the FCC (2010) established four principles for what they described as open internet:

- Customers' access to internet content is their choice.
- Considering the needs of law enforcement, customers' applications are permitted.

- Customers can choose what devices to connect to the Internet within legal limits.
- Customers can choose their content, services, and application providers.

These principles morphed into the *FCC Open Internet Order 2010*, a regulation that expanded on these principles to form a concept known as net neutrality (Federal Communications Commission, 2010). The three basic rules put into place by this order are:

1. Transparency: Fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and terms and conditions of their broadband services.
2. No blocking: Fixed broadband providers may not block lawful content, applications, services, or non-harmful devices; mobile broadband providers may not block lawful websites or block applications that compete with their voice or video telephony services.
3. No unreasonable discrimination: Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic. (p. 2)

In contrast to the United States, the Communist Party of China began a campaign on internet censorship in the 2000s that continues today (Congressional Executive Commission, 2011). Throughout the decade, China's leadership implemented laws and policies limiting internet access and increasing penalties for violations (Congressional Executive Commission, 2011). They took control of ISPs in the country as part of this process. It started in 2000 when Order No. 292 began content restriction through ISPs, giving the government access to any information they wished (Library of Congress Archives, 2004). In 2011, China was described as the most repressive country with its arrests and imprisonment of citizens for misusing the Internet (Congressional Executive Commission, 2011).

The number of ISP offerings in the 2000s changed through multiple mergers, including forming the DIRECTTV Group in 2003 after News Corps purchased Hughes Network Systems and DIRECTV (Ahrens, 2003). In 2005, Hughes Network Systems was sold to SkyTerra, which subsequently divested and became HughesNet (Los Angeles Business Journal, 2005). As mentioned in the satellite history section of this review, 2004 saw the first GEO satellite with enhanced throughput using the K_a band (Doan et al., 2004). This trend continued with multiple launches throughout the 2000s, allowing ISPs to offer higher bandwidth to more customers globally.

As the Internet grew in the 2000s, the threats to its users also (Middleton, 2017). The Center for Strategic and International Studies (2022) stated that in 2003, Chinese hackers gained access and stole nuclear weapons design and test data from the United States Naval Air Weapons Station China Lake. Another significant event occurred in 2006 when China stole 20 terabytes of data from the United States Department of Defense (Center for Strategic and International Studies, 2022). These threats continued throughout the decade, with attacks gaining sophistication and scale (Middleton, 2017). For example, in 2009, hackers attacked Israeli government websites from at least 5 million computers, causing significant disruption (Center for Strategic and International Studies, 2022).

Non-governmental entities such as corporations were also targeted during this time. For example, in 2001, a DoS attack against numerous online corporations was committed by a 15-year-old student called Mafiaboy (Geers, 2011). Damage estimates for this single attack totaled over $1 billion (Geers, 2011). In 2005, Chinese hackers stole NASA Space Shuttle data from Lockheed Martin and Boeing networks (Center for Strategic and International Studies, 2022). In 2008, United States companies ConocoPhillips, Marathon Oil, and ExxonMobil were hacked,

and sensitive data were stolen with an estimated loss of millions of dollars (Center for Strategic and International Studies, 2022).

Computer worms continued to grow, causing increased damage throughout the Internet. In 2001, the ILOVEYOU worm was released, infecting millions of users running Microsoft's Outlook, an email client for Windows computers (Committee on Government Reform, 2001). It operated like the Morris worm, using the recipients' address book to send many emails worldwide. It originated in the Philippines, and the creator was never charged since there was no local law against it (Grabosky, 2007). The Committee on Government Reform (2001) estimated this event's damage to be $8 billion. Code Red I and II were also released in 2001 and attacked over a million computers running a Microsoft website application called Internet Information Services (Committee on Government Reform, 2001). The trend continued throughout the 2000s, with MyDoom causing the most significant damage in 2004, estimated at $38 billion (Gerencer, 2020). It also relied on email to propagate, causing what is known as a distributed DoS (DDoS) attack against websites worldwide (Conrath, 2004). Internet and satellite technology and use continued to grow throughout the 2010s. However, the advancement most relevant to this study was the combination of the two in the emergence of the LEO satellite internet market.

LEO Satellite Internet Emergence: 1998–2017

Iridium was the first company to offer internet access via LEO satellites, and it did this in 1998 (Evans et al., 2011). It provided maximum speeds of 2.4 Kb/s through its LEO constellation of 66 satellites. The system was initially designed for satellite phone operation and only transmitted data at very low speeds (Yu & Qian, 2010). Iridium used satellite relays and ground stations to communicate, which improved speed compared to satellites operating in GEO due to latency (Yu & Qian, 2010). Ultimately, Iridium was a financial failure, with the company

filing for bankruptcy in 1999. Yu and Qian (2010) mentioned that this was due to the high launch cost, integrated circuit reliability, and maintenance costs. According to Iridium (2022), the company was reorganized in 2001, and under new ownership, continued to offer services using existing satellites until 2017. However, service was significantly degraded because most of the original constellation was no longer in service.

Globalstar, whose service went live in February 2000, also provided internet access (Evans et al., 2011). Like Iridium, Globalstar was designed with the primary use case of satellite telephony. It also provided system users access to the Internet at speeds of 9.6 Kb/s (Evans et al., 2011). A constellation of 48 satellites operating at an altitude of 1,414 km made Globalstar possible (Garrity & Husar, 2021). Although still in operation today, the company filed for bankruptcy in 2003 due to high operating costs and a limited user base and was reorganized (Evans et al., 2011).

Iridium and Globalstar's failures proved what LEO constellations' skeptics stated during this timeframe (Garrity & Husar, 2021). Garrity and Husar (2021) stated that hundreds or thousands of satellites are needed to achieve global and robust coverage. The financial burden of this effort, coupled with limited demand for services, will lead to the ultimate demise of early efforts. In addition, the connection speed of these early services was unable to match internet land-based ISPs that offered speeds of up to 56 Kb/s (Saif et al., 2007).

In 2004, a GEO satellite was successfully launched, utilizing the K_a band to gain enhanced throughput (Doan et al., 2004). High-speed access comparable to land-based broadband became a reality, with Viasat and Wildblue being the first to offer these services with GEO satellites (Weiss, 2004). With subsequent launches of the same technology, internet access via GEO proliferated, with services aimed primarily at rural locations unable to use land-based

services worldwide (Miller, 2017). The use of the K_a band was deployed to LEO satellites in the 2000s, but it was not until 2017 that companies began to attempt once again to provide LEO satellite internet access on a large scale.

Current Findings

As previously discussed, data used for this section were limited to those published between February 2017 and February 2022, primarily from peer-reviewed sources. An exception was made due to the ever-changing LEO space to include websites and magazine articles. Appendix A shows that six topic areas were covered under LEO satellite internet and internet end-user threats. The primary goal of this section was to review the current literature on the LEO satellite internet and potential cybersecurity threats. It further narrows on Starlink to identify a potential gap in the literature on specific cybersecurity threats to its primary user base—rural America.

Current LEO Status

Four leading companies are participating in the current LEO satellite internet market (Garrity & Husar, 2021). Starlink, Lightspeed, Kuiper, and OneWeb are in the process of building constellations, with Starlink currently offering commercial services in a non-beta or testing phase. Table 2 shows each product's current number of deployed, approved, and projected satellites. It also details the number of active customers and capital expenditures per product. As the only commercial product with an active roll-out and customer base, Starlink was chosen for this study in order for treatment to occur. Additionally, Starlink was awarded $885.5 million in United States Government subsidiaries in 2020 to support a program designed to bring broadband offerings to the unserved, mainly rural areas of the United States (Federal Communications Commission, 2020b).

Table 2

LEO Satellite Internet Providers

Characteristic	Starlink	OneWeb	Lightspeed	Kuiper
Satellites in Orbit	1,469	394	298	0
Approved per Current Regulation	11,943	648	298	3236
Total Satellites Planned	30,000	6372	1373	7774
Customer Count	145,000	0	0	0
Capital Expense	$30 Bil	$2.7 Bil	$5 Bil	$10 Bil

Note: Data from multiple sources: (Brodkin, 2018); (Federal Communications Commission, 2021b); (OneWeb, 2021); (Sheetz, 2022); (Sheetz, 2021c); (Sheetz, 2021d); (Telesat, 2020); (Wall, 2021).

Starlink Specifications

Manulis et al. (2021) state that LEO constellations have three distinct segments that interoperate to function, including Starlink. The space segment contains satellites launched into orbit; the ground segment comprises launch and recovery vehicles, stations, and associated infrastructure; and the user segment comprises each location's receivers, cabling, and router (Manulis et al., 2021).

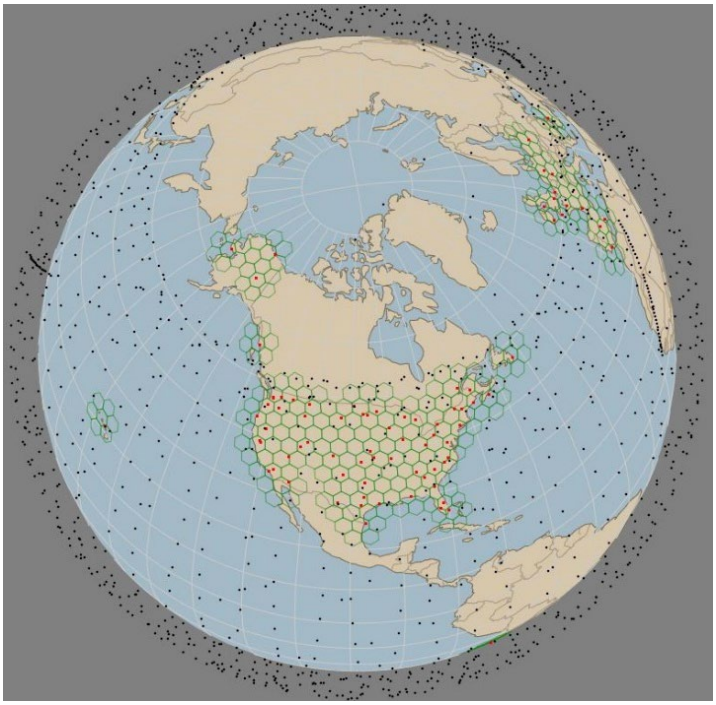
Starlink's space segment comprises 1,469 satellites operating in LEO at or below 580 km per FCC order (Federal Communications Commission, 2021b). Each satellite operates within the K_u and K_a bands, with frequencies in the ranges of "10.7–12.7 GHz, 13.85–14.5 GHz, 17.8–18.6 GHz, 18.8–19.3 GHz, 27.5–29.1 GHz, and 29.5–30 GHz" (Federal Communications Commission, 2021b, p. 3). The Space Exploration Technologies Corporation (2021) details six individual links used to communicate between the end-user equipment, the ground station, and the satellite. They are the user downlink, user uplink, gateway downlink, gateway uplink, and

downlink and uplink used for telemetry, tracking, and command. A report by the FCC (2021c) concluded that Starlink's multi-phased antenna uses dynamic allocation technology to ensure continuous coverage for users with up to 20 Gb of total throughput per satellite.

According to FCC filings (2021b), Starlink's initial plans call for five different locations, known as shells, for the constellation. The first shell consists of 1,440 satellites operating at 550 km and a 53.0-degree inclination. The second consists of another 1,440 satellites operating at 540 km and a 53.2 inclination. The third, comprising 720 satellites, will be deployed at 570 km with a 70-degree inclination. The fourth shell, comprising 336 satellites, will be deployed at 560 km with a 97.6-degree inclination, and the fifth, comprising 172 satellites, will be deployed at 560 km with a 97.6 inclination. Due to their distance from Earth, each LEO satellite orbits approximately 16 times in 24 hours (The European Space Agency, 2020b). Although no official map of the Starlink constellation exists for public consumption, many non-SpaceX affiliates have produced websites and mobile applications for tracking purposes. Figure 9 indicates the current estimated coverage and location of Starlink satellites, focusing on the United States.

Figure 9

Starlink Coverage Map

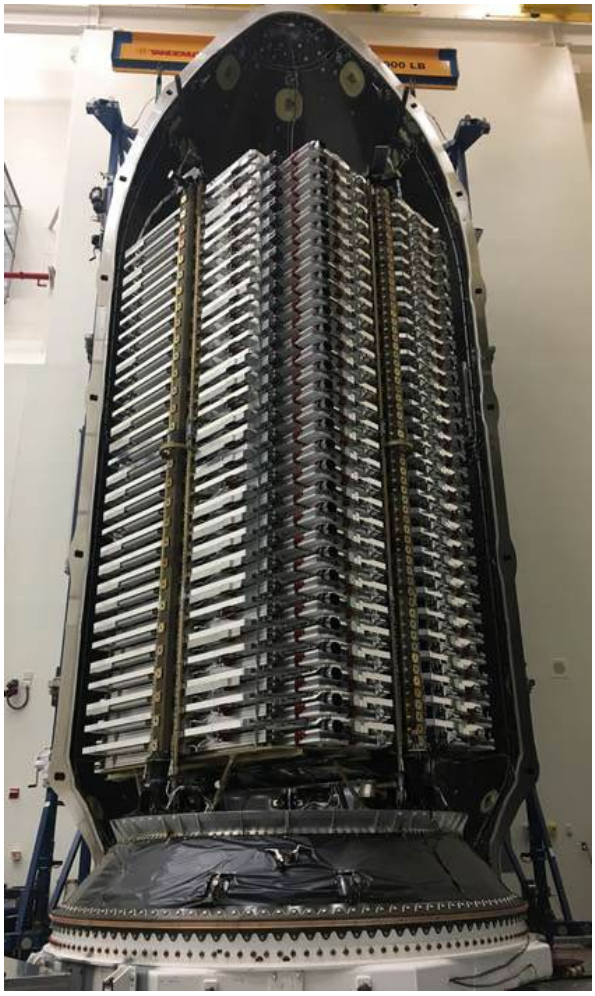


Note. A black dot represents an individual satellite, with red showing a ground station. From *Starlink Coverage Map* (2022). (https://satellitemap.space/?constellation=starlink) Reprinted with permission.

SpaceX, Starlink's parent company, operates the required infrastructure to launch and recover each satellite (SpaceX, 2022). Since 2018, SpaceX has successfully deployed Starlink satellites through 37 separate missions (SpaceX, 2022). The Falcon 9 multi-stage rocket has been used with reusable carbon for missions to protect the satellites before deployment (SpaceX, 2022). Each mission contained approximately 60 Starlink satellites (SpaceX, 2022). Figure 10 depicts satellites within a Falcon 9 fairing before launch.

Figure 10

Falcon 9 Fairing with Starlink Satellites



Note. From *First 60 @SpaceX starlink satellites loaded into falcon fairing. Tight fit*. (2019, May 11). (https://twitter.com/elonmusk/status/1127388838362378241). Reprinted with permission.

Starlink uses ground stations or gateways to connect each satellite to the terrestrial internet backbone. It does not provide public information on its gateways. However, it must submit a license application to the FCC in the United States before installation. This data shows that Starlink has 64 gateways throughout the United States (Federal Communications Commission, 2021b). Each gateway contains eight identical, active antennas authorized to transmit between 27.5 and 29.1 GHz and receives between 17.8–18.6 GHz and 18.8–19.3 GHz

(Federal Communications Commission, 2021b). SpaceX also surveys each location to ensure the uplink power flux density does not interfere with existing or planned radio signals (Federal Communications Commission, 2020b).

The user segment of Starlink contains a receiver, a router, and the accessories required for it to provide service (Starlink, 2022). The receiver has been shipped in two forms. The first was a circular dish weighing 16 lbs. and measuring 23.2 in diameter. The second generation and current dish shipping to new customers are rectangular, measuring 19” x 12” and weighing 9.2 lbs. (Starlink, 2022). The router has also shipped in two forms alongside each of the receivers. Both routers support 802.11a/b/g/n/ac wireless standards and only WPA2 or WPA3 for wireless security. The first generation has two antennas for wireless coverage, while the second has three (Starlink, 2022). They are shipped as a kit to end-users with instructions for setup and use (Starlink, 2022).

LEO Satellite Segment Threats

Within each of the segments for LEO satellite internet exists specific threats that security experts have identified (Cao et al., 2020; Scanlan et al., 2019). Published literature on space, ground, and user segments was reviewed to determine what gaps may exist, particularly in end-user security threats. Manulis et al. (2021) concluded that innovation and recent advancements in satellite technology leave many information security challenges yet to be researched and resolved.

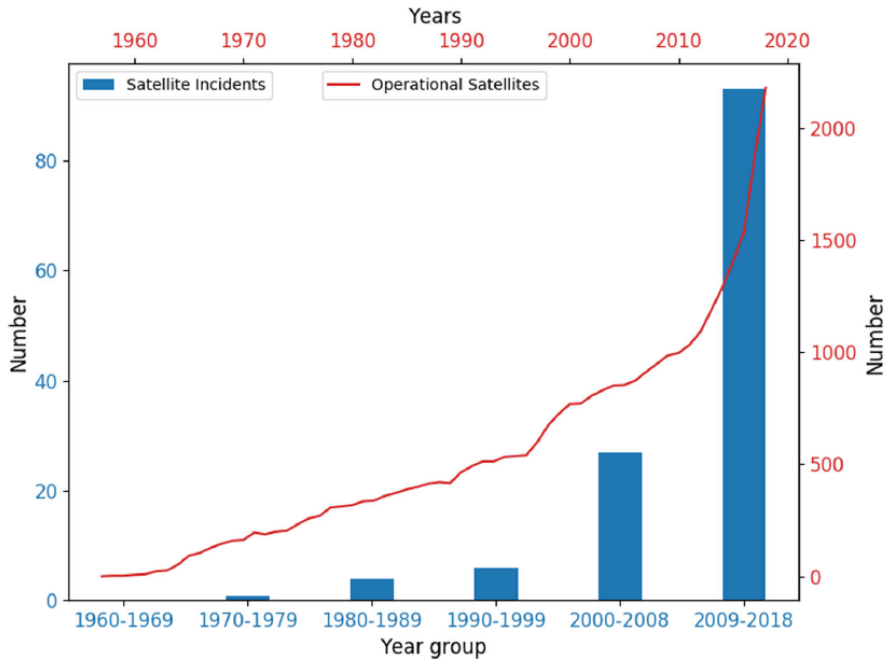
Space Segment

The space segment, as discussed previously, comprises satellites. Manulis et al. (2021) mentioned that vulnerabilities within the hardware and software contained within these devices are a significant threat. These vulnerabilities may be exploited to disrupt providers' ability to

serve their end customers (Manulis et al., 2021). One example is jamming, where small malformed packets are sent to a radio transmitter on the satellite, causing a DoS attack (Manulis et al., 2021). Furthermore, many space systems, including satellites, are considered critical infrastructures for many industries (Falco, 2018). For example, an attacker seeking to compromise an e-commerce business may infiltrate several systems the organization uses to run its operations. Falco (2018) argues that a more straightforward route is to attack the connectivity method for users and the business, a space-based ISP. Figure 11 shows how attacks have increased alongside satellite counts from 1960 to 2018 (Manulis et al., 2021). Trend data indicates this will continue as the number of satellites increases.

Figure 11

Satellite Cybersecurity Incidents



Note. From cyber security in new space, by Manulis, M. et al., 2021. *International Journal of Information Security, 20*, 287–311 (https://doi.org/10.1007/s10207-020-00503-w). Reprinted with permission.

Satellites also contain thousands of highly specialized components from many manufacturers (Falco, 2018). This lack of supply-chain control allows a nefarious actor to comprise a component via a hardware or software vulnerability (Falco, 2018). Similarly, Starlink manufactures its satellites using numerous Taiwanese suppliers, such as Elite Material Co., Parpro Taiwan, and Huatong Computer Co., each participating in circuit board production (Hung, 2021). Additionally, due to their relatively small size, LEO satellites have limited storage and computing power, leading to a reliance on physical measures to secure components and not on traditional security algorithms using software (Yue et al., 2022).

Another threat within this segment is space debris (Yue et al., 2022). Frequent launches, combined with an ever-increasing number of satellites operating in LEO, provide a possibility of debris causing service disruption. This threat occurred in 2009 when an Iridium satellite collided with a Russian military satellite in LEO (Brito et al., 2013). This event, at 800 km, generated a debris field from 180 km to 1700 km, with approximately 1,685 individual objects (Brito et al., 2013). Starlink has claimed, through its filing with the FCC, that its satellites potentially may track debris and avoid it in an automated fashion without human involvement (Federal Communications Commission, 2021b).

Signal interference is another threat that must be examined (Cao et al., 2020). Unlike jamming, where malformed data is received, interference occurs when a satellite receives a large amount of data on the same frequency band (Cao et al., 2020). This data may potentially overwhelm a single satellite, rendering legitimate connections unusable. Fixed high-power transmitters are typically used to perform these attacks (Cao et al., 2020). Compared with GEO offerings, LEO satellite ISPs are less vulnerable to signal interface due to their orbit speed. With

each satellite rotating the earth approximately 16 times per day, the number of times a single satellite can be affected is limited (The European Space Agency, 2020b).

Ground Segment

The ground segment of LEO satellite internet contains infrastructure that is physically more susceptible to attack than space components (Manulis et al., 2021). Gaining access to this infrastructure may lead to tampering or destruction, which may have a widespread effect on the ISP's service offering (Manulis et al., 2021). Command and control, monitoring, and user internet traffic back to Earth are performed through the links between the ground stations and satellites (Space Exploration Technologies Corporation, 2021). A well-known example of exploitation against these links occurred in 2015 when a Russian-based group, Turla, used a ground antenna to intercept the link between a ground station and a GEO satellite (Kaspersky, 2021). They used the data obtained to steal user IP addresses which they used to appear as legitimate traffic while they hid cyber-espionage operations against other countries (Kaspersky, 2021).

Manulis et al. (2021) also mentioned that each ground station for LEO satellite internet systems is connected to a network that ultimately connects to the terrestrial Internet. Well-known exploitations of these networks are also a risk, including software and hardware vulnerabilities (Manulis et al., 2021). Like those within the space segment, supply chain attacks are also a threat, with unique components and multiple companies participating in manufacturing (Manulis et al., 2021).

User Segment

User segment threats include software and hardware vulnerabilities and physical interaction with infrastructure (Cao et al., 2020; Manulis et al., 2021). As previously mentioned

in the space portion of this section, the user segment devices also utilize multiple suppliers. For example, the router shipped to Starlink customers is manufactured by a third-party company named Wistron NeWeb Corporation, based in Taiwan (Federal Communications Commission, 2020c). The same supply chain issues observed with satellite components also exist with the end-user components (Falco, 2018).

Eavesdropping is another threat that must be examined with LEO satellite communication (Yue et al., 2022). Pavur and James (2020) mentioned that eavesdropping is performed by imitating a legitimate network user. Using this method, an attacker may send malicious data to disrupt a satellite system. Broadband internet delivered via this method is particularly susceptible due to the number of users and associated equipment (Pavur & James, 2020). These threats exist due to the lack of encryption in the connection between the user equipment and satellites (Cao et al., 2020). Possible attack methods described by Cao et al. (2020) include the following:

> 1. The attacker uses a kind of satellite data receiving card to steal data, which is similar to but cheaper than the computer network card.
> 2. The attacker makes use of equipment abandoned by manufacturers to perform network attacks.
> 3. The attacker uses the VLEO or LEO satellite in the overseas satellite constellation to eavesdrop on the service data on the user and feeder links of the domestic satellite system.
> 4. If the satellite constellation built in a country has an ISL which uses microwave communication, the attacker can control a foreign satellite to come as close to the target satellite as possible to implement data eavesdropping. (p. 201)

Full-stream encryption of each link is the solution, but the overhead needed outweighs the advantages for many satellite internet providers (Yue et al., 2022). However, Starlink uses hardware-based encryption on user link equipment to ensure its users' privacy and mitigate eavesdropping attacks (Starlink, 2022).

Jamming is another threat to LEO satellite internet terminals; however, unlike its threat to the space segment, it is limited to single links, which may affect thousands of customers. A high-profile event occurred on March 5, 2022, when Starlink terminals shipped to Ukraine were jammed by an unknown source (Foust & Berger, 2022). These terminals were sent in response to Russia's shutdown of terrestrial ISPs and the GEO ISP Viasat service due to cyber events (Foust & Berger, 2022). Although no specifics were provided, Starlink responded by pushing a software update to resist the jamming events on the same day (Foust & Berger, 2022).

To combat these threats, the Cybersecurity and Infrastructure Security Agency (2020) released guidelines for end-users to reduce the risk of exploitation due to vulnerabilities. The guidelines include the following:

- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band (OoB) network management.
- Validate integrity of hardware and software. (Cybersecurity & Infrastructure Security Agency, 2020, p. 1)

SpaceX has set up a program for the information security community to address a few of these concerns by submitting vulnerabilities that potentially may exploit their Starlink product,

including the user segment router and dish (Bugcrowd, 2022). Currently, 29 vulnerabilities have been found using this method (Bugcrowd, 2022).

Internet End-User Threats

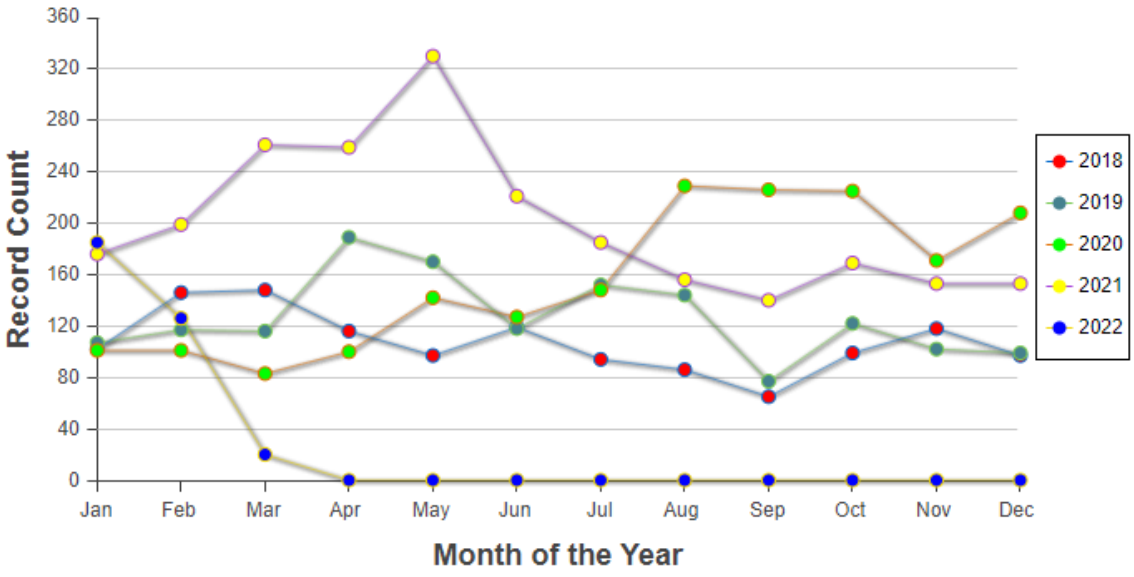
In addition to LEO satellite-specific threats, internet use is associated with risks (Geers, 2011). This section details current findings related to data breaches, identity theft, reputational harm, malware, and viruses. Each section focuses on the impact on end-users of the internet.

Data Breaches

The International Organization for Standardization (2015) defined a data breach as losing, changing, or destroying protected data. As discussed in Chapter 1, data breaches have increased drastically over the past decade, with a 36% increase in the United States in 2020 (North Carolina Department of Justice, 2021). Figure 12 from the Identity Theft Resource Center (2022) shows reported data breaches in millions based on the number of records stolen globally over the past five years until March 2022.

Figure 12

Data Breach Trends



Note. From *Data breach trends,* by Identity Theft Resource Center, 2022. (https://notified.idtheftcenter.org/s). Reprinted with permission.

The most significant recent event occurred in 2017 when Equifax was the target of a data breach, where 147 million United States citizens were affected (Spinello, 2021). The data stolen included personally identifiable information such as customers' names, addresses, and social security numbers (Dinger & Wade, 2019). The attackers used the Internet as a transport mechanism, exploiting a vulnerability in Equifax's online dispute system (Spinello, 2021). This event occurred after several significant data breaches, including the theft of millions of records from Yahoo!, LinkedIn, Target, and Home Depot, had been reported (Dinger & Wade, 2019). Had this breach occurred before those events, the reaction from a customer and shareholder standpoint may have been more impacting than it was (Dinger & Wade, 2019). As shown in Figure 12, millions of customers are affected by data breaches every year, with an estimated 43% of companies operating on the Internet experiencing a breach of some type (Dinger & Wade, 2019). As this trend continues, Dinger and Wade (2019) argue that customers have become desensitized to stealing their personal information.

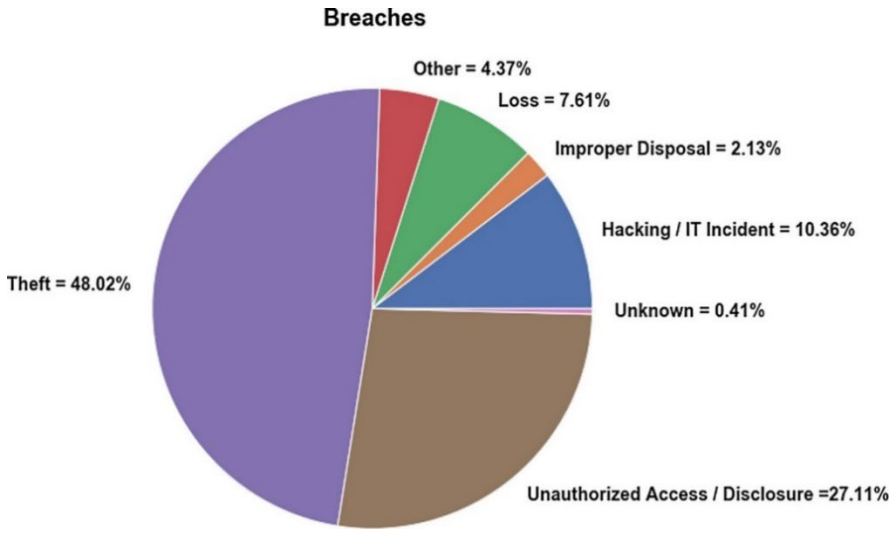
Spinello (2021) argues that data breaches show a lack of cybersecurity control by the business where they occur. These controls include proper data encryption, access control, network, and endpoint security (Spinello, 2021). Developing a framework adhering to the basic cybersecurity principles of confidentiality, integrity, and availability is a method that Spinello (2021) details to achieve these controls. Lundgren and Moller (2019) describe confidentiality as ensuring that data is only available and accessed by authorized individuals; they also define integrity in this context as how accurate and complete the data being held by the entity is and

availability as ensuring that data is only in a usable state for users that have been authenticated and authorized.

Hughes-Lartey et al. (2021) detailed the causes of data breaches in their study. They categorized breaches reported from 2009 to 2017 as either theft, loss, improper disposal, hacking, unauthorized access, or unknown. They describe theft as stolen physical items, including USB drives, laptops, backup disks, and more, and loss is when data is misplaced by an employee and compromised (Hughes-Lartey et al., 2021). They also described improper disposal as poor handling of sensitive data by employees. For example, customer records that may have been destroyed electronically are left on a hard drive for a nefarious actor to exploit. Hacking and unauthorized access are similar in removing data electronically (Hughes-Lartey et al., 2021). Hacking involves exploiting security weaknesses, where unauthorized access is typically gained through an employee with more access than required to perform their job (Hughes-Lartey et al., 2021). Other and unknown are breaches where the cause was never found or cannot be classified into other listed categories (Hughes-Lartey et al., 2021). Figure 13 shows these causes in percentages.

Figure 13

Data Breach Causes



Note. Human factor, a critical weak point in the information security of an organization's Internet of things, by Hughes-Lartey et al., 2021. *Heliyon*, *7*(3), e06522 (https://doi.org/10.1016/j.heliyon.2021.e06522). Reprinted with permission.

Janjarasjit and Chan (2021) studied the effects of data breaches on victims and possible preventative measures. They determined that victims experienced emotional distress after a breach announcement; this phenomenon was associated with a victim's thoughts on whether a perpetrator may feel shame, guilt, or regret for their actions (Janjarasjit & Chan, 2021). They also argued that users are the weakest link in the chain of security protection and that a lack of awareness and poor security practices increase the probability of a data breach (Janjarasjit & Chan, 2021).

Identity Theft

As discussed in Chapter 1, the United States Department of Justice (2020) defines identity theft as the wrongful possession of a victim's data that may be used for financial gain. The Federal Bureau of Investigation reported a $3.5 billion loss for United States citizens in

2019 alone (Federal Bureau of Investigation, 2019). This section details the leading causative factors of identity theft and preventive measures.

Gupta and Kumar (2020) describe four factors that lead to identity theft: technological, economic, political, and social. Technological factors involve end-users not taking safety measures to prevent identity theft; these measures include only using secure internet websites to conduct personal business and not saving usernames and passwords within a browser (Gupta & Kumar, 2020). Economic and political factors also contribute to identity theft. Gupta and Kumar (2020) gave the example of illegal immigrants purchasing stolen information for a new identity. The social factors involve the increasing use of the Internet by developing countries for everyday life; for example, victims who do not safeguard their use of internet social media are often targets of theft (Gupta & Kumar, 2020).

Gupta and Kumar (2020) recommended several preventive methods for identity theft for users and organizations with personal data. These include:

1. Do not share or disclose your personal information to anyone.
2. Never disclose any personal information to anyone, even if the other party initiated the conversation.
3. Regularly check your credit report, and if not regularly, then at least once a year.
4. Destroy every document that can be used against you.
5. Use different passwords, and make these passwords durable and protective.
6. Companies would keep an eye on the safety precautions that they are taking into account. Their network security should be firm, and incidences of a security breach should be taken seriously and divulged in time to users and employees. (p. 904-905)

In a study by Zou et al. (2020), prevention methods for internet users against identity theft were researched. Thirty recommendations by cybersecurity experts were analyzed for effectiveness by a survey of 902 internet users. These recommendations included anti-virus software, password managers, automatic software updates, and secure browsing validation. (Zou et al., 2020). Zou et al. (2020) concluded that the recommendations made by cybersecurity experts need to be more user-friendly. For example, they stated that most of the password management tools on the market are difficult to use and require multiple clicks and steps to retrieve data. They found that identity theft protection services were limited, with only 6% of the research participants paying a one-time subscription membership. Demographics were also analyzed, with males, with a lower household income and a higher education level showing a higher adoption rate for identity theft prevention methods.

Burnes et al. (2020) studied additional risk factors and protective measures against identity theft to determine what behaviors led to increased victimization. Data from the United States Department of Justice were used. A seven-question survey related to internet protection behavior practices was sent to victims who reported an identity theft over two years. They found that victims who practiced protective measures such as using unique passwords and frequently changing them were 25%–35% less likely to experience identity theft (Burnes et al., 2020). They also found that Caucasian females living in urban areas were likelier to fall victim to theft. In addition, those who frequently made e-commerce purchases had increased odds of their personal bank account and credit gift card information being stolen as part of the identity theft (Burnes et al., 2020).

Reputational Harm

As mentioned in Chapter 1, reputational harm is a negative shift in an individual's perception due to an outside source (Agrafiotis et al., 2018). Agrafiotis et al. (2018) concluded that reputational harm results from cybersecurity events such as a data breach, where personal information is stolen. Other types of harm, such as physical, economic, psychological, and social, may also stem from data breach events (Agrafiotis et al., 2018).

Hamilton (2017) stated that the consequences of reputational harm might include damage to friendships, depression, job loss, and even suicide. He also argues that internet accessibility is prominent in the possible damage. For example, "fully online individuals with substantive and long histories of social media presence may defeat reputational and historical harms by simply continuing to create content such that negative search results decrease in proportion to in their social media presence" (Hamilton, 2017, p. 181).

Solove and Citron (2018) examined the legal implications of a data breach and the reputational harm to both business and individual victims. They found that the United States court system passes inconsistent judgments when victims allege that a corporation allowed their data to be stolen. One case, which reached the United States Supreme Court, was examined. In Spokeo v. Robins, the court noted that the risk of injury, even if intangible, is enough to prove reputational harm (Solove & Citron, 2018). Solove and Citron (2018) also argued that data does not exist independently once compromised. In other words, the collection of variable data can be combined to increase the possibility of harm to the victim.

Malware and Viruses

Zhong et al. (2022) defined malware and viruses as software designed to cause harm to users, applications, or hardware. As shown in the historical overview section of this chapter, the

proliferation of malware and viruses has grown since the inception of the Internet (Middleton, 2017). Alenezi et al. (2020) described malware's evolution as being in its fifth and current phase.

Before the 2010s, malware, and viruses were primarily created by individuals, focusing on organizations and personal devices (Alenezi et al., 2020). After 2010, militaries and other government-backed entities began to develop tools focused on severe damage and data loss (Alenezi et al., 2020). Alenezi et al. (2022) defined these attacks as advanced persistent threats (APTs), and Hofer-Schmitz et al. (2021) further described APTs as follows:

- Advanced: The attacks are goal-oriented and performed by highly organized, advanced, and well-resourced attacker groups using adaptive tools.
- Persistent: The goal of these attacks is not rapid damage. Such attacks are persistent and the attackers tend to stay undetected as long as possible in the system to gain as much information as possible.
- Threat: The goal of these attacks is usually to get valuable data, e.g., sensitive data and strategic or product information. Therefore, the attacks usually lead to great damage for the victims. (p. 1)

Hofer-Schmitz et al. (2021) demonstrated the impact of this type of malware on the users affected and the damage caused. For example, Capitol One was a victim of an APT in 2019, where 15 million customer records were stolen containing credit limits, payments, balances, and personal information (Hofer-Schmitz et al., 2021). Another recent attack using this method was launched against FireEye, an internet security company (Teodorescu, 2022). The Russian government-backed group APT29 gained access via a supply-chain weakness, exposing internal data and threatening the security of networks and FireEye products' global users (Teodorescu, 2022).

Chapter Summary

A detailed review of the historical and current literature was performed, and several studies on the current LEO status, LEO segment threats, data breaches, identity theft, and reputational harm were found. Manulis et al. (2021) described the unique corporations participating in LEO satellite internet and reviewed the technology. The FCC (2021a) also provided specific information on implementing the SpaceX product Starlink. The studies conducted by Cao et al. (2020) and Yue et al. (2022) provided vital information regarding LEO segment threats, and Hughes-Lartey et al. (2021) covered the causes and outcomes of data breaches, with Gupta and Kumar (2020) studying the factors that lead to identity theft for internet users. Furthermore, Solove and Citron (2018) covered the legal ramifications of reputational harm to end users, and Alenezi et al. (2022) described the advancement of malware and viruses in APTs.

Chapter Conclusion

This review covered the historical and current literature on satellite systems, the Internet, LEO segment threats, data breaches, identity theft, reputational harm, malware, and viruses. The eight steps detailed in the SLR methodology section were utilized throughout the review, and it was determined that an extant gap exists in the literature. No significant work was found detailing the cybersecurity risks associated with LEO satellite internet use for end-users, specifically Starlink. Chapter 3 details the research method used to answer the three research questions. It also covers the appropriateness of the present study's design, population, sampling, data collection procedures, instrumentation, validity, and data analysis.

CHAPTER 3: METHOD

This quantitative study utilized a quasi-experiment to examine the cause-and-effect relationship between Starlink and end-user cybersecurity risk. A pre-test and post-test design with a control group was used. Chapter 2 reviewed the history and current literature on satellite systems, the Internet, LEO segment threats, data breaches, identity theft, and reputational harm. A gap in the literature specific to Starlink end-user cybersecurity risk was found.

Chapter 3 detailed the research method used to answer the three research questions in Chapter 1. Chapter 3 covered the appropriateness of design, population, sampling, data collection procedures, instrumentation, validity, and data analysis for this study. The sections contributed to the appropriateness of the research methodology and design chosen.

This quantitative study utilized a quasi-experiment design to examine the cause-and-effect relationship between Starlink and end-user cybersecurity risk. A pre-and post-test design with a control group was used. This study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite Internet upon rural American customers. Chapter 2 thoroughly reviewed the historical and current literature on satellite systems, the Internet, LEO segment threats, data breaches, identity theft, and reputational harm.

Chapter 3 details the research method used to answer the three research questions outlined in Chapter 1. It covers the appropriateness of design, population, sampling, data collection procedures, instrumentation, validity, and data analysis for this study. Each section contributes to the appropriateness of the chosen research methodology and design.

Research Method, Design Appropriateness, and Rationale

Creswell and Guetterman (2019) described quantitative studies as static and valuable for investigating relationships between factors; in contrast, they described qualitative studies as involving open-ended questions. Mixed-methods research uses quantitative and qualitative methods to answer questions (Edmonds & Kennedy, 2016). Creswell (2012) further described quantitative research as fulfilling a need for the variable relationship definition. The evaluation criteria must be standard to ensure an unbiased data analysis (Creswell, 2012; Creswell & Creswell, 2018). In addition, when dealing with human subjects, the data must be numeric, using identical instrumentation and questions (Creswell, 2012). This study determines if a relationship exists between the installation and use of Starlink and cybersecurity risks using analytical data; this makes the quantitative method the most appropriate for this study.

As mentioned in Chapter 1, a pre-and post-test experiment was utilized in this quantitative study. The study design was quasi-experimental. Salkind (2018) described quasi-experimental designs as having a single but significant difference compared to pre- and true-experimental designs. He said that in quasi-experimental designs, the "hypothesized cause of differences you might observe between groups has already occurred" (Salkind, 2018, p. 194). A crucial assumption in this study was that group assignments had already occurred; therefore, a quasi-experimental design was used to determine if a cause-and-effect relationship exists between the use of Starlink and cybersecurity risks.

In addition to the quasi-experimental design, pre- and true-experimental designs were investigated. The non-experimental design was not considered as; according to Salkind (2018), it is qualitative. Frey (2018) mentioned that pre-experimental designs are used to explore the

benefits of further research. As established in Chapter 2, there is evidence of a gap in the literature, showing a need for further research and making a pre-experiment inappropriate.

Salkind (2018) described true-experimental designs as having randomization of treatment, with a minimum of one independent and dependent variable present. For this study, the treatment administration was unable to be controlled; many factors, including Starlink's deployment schedule, manufacturing delays, and SpaceX launch issues, played into treatment dates. Although the study has an independent and dependent variable, the randomization needed for a true-experimental design makes it an inappropriate choice.

The pre-and post-test control group design was chosen based on Salkind's (2018) recommendation that both participants be equal at the start of an experiment. Salkind further stated that the difference between the pre-and post-test directly results from the treatment or lack thereof (Salkind, 2018). For this study, the participants were equal before the start of the experiment based on their pre-orders for Starlink. The installation and use of Starlink was the independent variable administered as the treatment. The dependent variables were the occurrence rates of identity theft, data breaches, reputational harm, and malware and viruses.

Population, Sampling, Instrumentation, and Data Collection Procedures

Population

Creswell (2014) defines a population as a group with common characteristics. Creswell and Guetterman (2019) filter this to a targeted population, representing a small percentage overall. This study targeted rural Americans who had pre-ordered but had not yet installed SpaceX's Starlink LEO satellite internet product. Sheetz (2021b) found that 500,000 pre-orders had been submitted for Starlink as of June 2021. The total sample population for this study was 868; this figure represents those who participated in the pre-test, including the pilot group of 17.

The final number of valid participants who participated in the pre-and post-test was 46. The control group consisted of 19 participants. Creswell and Creswell (2018) explained that this group is vital when performing quasi-experimental research. All participants stated they were of legal age and had pre-ordered the Starlink product. The initial goal was to have 50 states represented by at least one participant. Although this was not reached, representation from 22 states was achieved, with a sample size to collect empirical data from the sample and control groups.

Sampling

Once the specific population was found, sampling commenced. Creswell (2012) described quantitative research sampling as using the probability technique, where each member of the chosen population has a chance of being selected for treatment. This study ensured that each participant had pre-ordered but not installed or used Starlink. The first question asked on the survey was whether a pre-order had been placed, and any potential participants who answered "no" were not permitted to proceed.

Neuman (2013) detailed four types of probability sampling to be considered by a researcher. First is cluster sampling, used when a large area needs to be researched, with units selected randomly and samples pulled from each unit (Neuman, 2013). The second is systematic sampling, which uses a calculated interval to create the desired population (Neuman, 2013). Third is stratified sampling, which identifies categories and pulls samples from each until reaching the target number (Neuman, 2013). Last is simple sampling, which uses an entirely random process, usually via a computer program. None of these four sampling methods was appropriate for this study. Frey (2018) detailed the judgmental technique in which a researcher

deliberately selects the subjects that best answer the research questions posed. This technique was found to be best suited for this study.

Instrumentation

The instrumentation used to collect data to determine the specific effects of Starlink on the cybersecurity risk of end-users was a web-based survey. The application used to host the pre- and post-test surveys was surveymonkey.com. This application was chosen based on its high-level security, usability, and ease of data analysis criteria. The researcher also observed the successful use of this application in numerous published dissertations and research.

Concerning the security and confidentiality of the data collected, surveymonkey.com (2022) stated as follows:

> All your respondents' information is securely stored in our SOC 2 accredited data centers that adhere to security and technical best practices. We ensure that collected data is transmitted over a secure HTTPS connection, and user logins are protected via TLS. Data at rest is encrypted using industry-standard encryption algorithms and strength. (pg. 2)

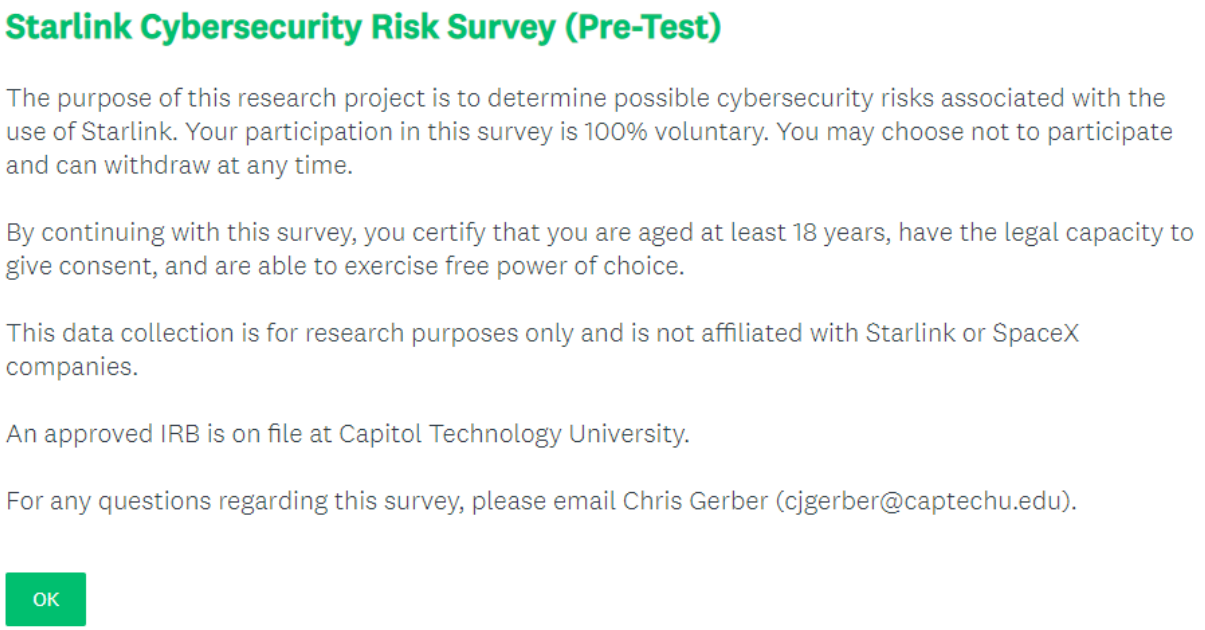
The researcher used a strong username and password combination and multi-factor authentication to limit access to the source data.

Data Collection

Neuman (2013) described consent as vital before conducting research involving a human subject. At a minimum, a researcher must (a) gain consent prior to data collection, (b) never cause harm, (c) protect the data at all costs, and (d) never release harmful data about a participant (Neuman, 2013). The consent statement for this research was placed at the beginning of the pre- and post-survey, with each participant accepting the terms before starting. Figure 14 shows the verbiage approved by the institutional review board (IRB) at Capitol Technology University.

Figure 10

Prior Consent



The data collected included an email address, zip code, number of household members, and a series of questions to best answer the four research questions for this study. Each question was presented on a different screen to ensure that the end-user gave each question the right amount of focus. In addition, logic was built into the survey to display the next appropriate question based on their response. For example, if a participant stated yes to the question "*In the past 24 months, have you been a victim of identity theft,"* they were presented with the following question: "*How many incidents of identity theft have you experienced?"* The next question was skipped if they answered no to the first question. Appendices B and C show the pre- and post-survey questions and response types.

To determine the reliability of the quasi-experimental design and instrumentation, a pilot study was conducted with 17 participants. A separate survey was created containing questions identical to those in Appendix B, along with four additional questions geared towards feedback

on the instrumentation and preferences of the participants. Appendix C shows the additional questions posed. Advertisement for the pilot study was made in the same manner as described below, with only three Facebook groups used until over 15 responses was received. After obtaining the required responses, the survey link was disabled, and responses were collated for analysis.

Facebook, a social media platform based in the United States, was used for advertising for the participants (Meta Platforms, 2022). To encourage maximum participation by rural dwellers, the researcher joined two city Facebook groups for every state with a population of less than 50,000 between September 1, 2021, and October 25, 2021. Most of these groups required a purpose for membership to be stated before the group administrator approved. The researcher used the following statement for each request:

> *I am a college student looking to conduct research on rural communities in the US for my dissertation. I am located in Bentonville, Arkansas. I promise to only ask for members to complete a short survey in the future based on their Internet Access. Thanks, Chris Gerber.*

The researcher also joined Starlink groups geared towards those interested in the product to drive increased participation. In total, the researcher joined 104 groups for advertisement purposes. Compensation for participants was advertised via Facebook. For participants who completed both the pre-and post-survey, a $50 gift card for Amazon.com was offered for one winner drawn at random. The researcher used the following statement in a post to each Facebook group when attempting to recruit participants between October 26, 2021, and December 26, 2021:

My name is Chris Gerber, and I am conducting research for my doctorate in cybersecurity. If you live in the USA, have pre-ordered but not yet installed Starlink, I would love your help to gather data! I have a short survey that can be accessed here: https://www.surveymonkey.com/r/Z2GX7TW

Happy to answer any/all questions via PM. The survey will ask for your email address for a follow-up survey and Zip code for demographics. It shouldn't take more than 10 minutes of your time, and a $50 Walmart gift card will be given to a random participant. Thanks in advance!

Six months after the close of the pretest survey, on June 26, 2022, the follow-up email was sent to pre-test participants with the post-test survey website link. The researcher allowed 90 days for survey completion, with two reminders sent to participants who failed to respond promptly. Once responses were received, the researcher conducted the gift-card drawing on September 2, 2022, using Microsoft Excel's randomization software to choose the winner, who was notified via email, validated, and sent the card electronically.

Validity: Internal and External

Salkind (2018) defines internal validity as the sustenance and quality of a design to ensure that results are a unique representation of the independent variable change. Furthermore, different explanations for the outcome of an experiment will prove internal validity false (Salkind, 2018). Dimitrov and Rumrill (2003) listed the following as common factors that threaten to make an experiment invalid: “history, maturation, pretest effects, instruments, statistical regression toward the mean, differential selection of participants, mortality, and interactions of factors” (p. 159). They further described the pre-and post-test research design

with a control group, which this study employs, as having the factors of maturation and history, which are essential to consider.

Maturation is when a psychological or biological shift occurs between the pre- and post-tests and affects final scoring (Dimitrov & Rumrill, 2003). In this study, the dependent variable—cybersecurity risk occurrence rates—may have been affected by external changes to the human participants, which are unrelated to the installation and use of Starlink. For example, supposing treatment is received alongside a physical injury resulting in reduced psychological reasoning, it will be challenging to determine if the results are from the treatment or injury. Based on the questionnaire, this study assumed that participants retained the ability to recognize if a cybersecurity event had occurred. To ensure an understanding of the survey, the researcher added examples for each question related to the dependent variable. Appendices B and C show these examples.

History is when participants in a study have an occurrence in their life that affects their post-test scoring (Dimitrov & Rumrill, 2003). Wright (2001) explains that this phenomenon may significantly obscure results, and researchers must consider possible pre- and post-test occurrences. For this study, the duration between the two tests was six months to allow treatment for a portion of the participants. This duration was necessary due to circumstances outside the researcher's control, such as product delays and the contractual agreements between the end users and Starlink. The researcher's timeframe threatened internal validity, as unforeseen events may have changed the post-test results. Chapter 4 details the potential history-based effects that may have altered the results of this study.

Another essential item to consider with internal validity is selection bias. Pannucci and Wilkins (2010) define bias as any prejudiced decision made by a researcher that may affect the

outcome of a study. Selection bias relates to the participants chosen by the researcher (Pannucci & Wilkins, 2010). The population is not chosen randomly but rather with a potential outcome in mind based on a characteristic (Pannucci & Wilkins, 2010). For this study, the researcher only asked that participants be of legal age and have already placed a pre-order for Starlink. Participation was voluntary and open to anyone accessing the advertised publicly available survey.

External validity ensures that results are generalized outside the specific setting where the experiment was initially performed (Neuman, 2013). Creswell and Creswell (2018) detailed three critical threats to external validity: selection and treatment, setting and treatment, and history and treatment. They explained selection and treatment as the lack of generalizability within the groups participating in research, such as age, race, and socioeconomic background. To combat this threat in the present study, the researcher opened the survey to anyone accessing the URL and did not limit it to specific groups. As discussed in this chapter's population and sampling section, a targeted approach was used for advertising the survey but was only limited to those of legal age who had placed a pre-order for Starlink. Creswell (2012) explains setting and treatment as the inability of an experiment to generalize from the original location to another. This research took place wherever the participants chose, with the only setting requirement being a personal computer, phone, or another internet-connected device that was able to load and interact with the web-based survey. The threat of setting and treatment was averted due to these basic requirements. A history and treatment threat is when researchers generalize their results to the study's timeframe (Creswell & Creswell, 2018). This study may be conducted at any time if certain conditions are met, such as the participants needing to have ordered and not yet received their high-speed internet connection offered via LEO satellites.

Data Analysis

Data examined in this study, described in Chapter 4, include information from the control group and those who received the treatment. It is essential to note the differences between these two groups, as determining an increase or decrease in cybersecurity risk depends on the accuracy and completeness of the data obtained. The location of the participants in both groups is also pertinent, as this study focuses on the primary end-users of the product, which, as previously stated, were persons dwelling in rural America. Another critical piece of data analyzed was the duration of treatment administered to determine the effect on the survey results.

This study's pre-and post-test design provided the most crucial aspect of the data analysis—determining if the scoring changed between the two surveys and by what factor. These differences were analyzed using Microsoft Excel's charting feature to visualize the results. The control and treatment groups were examined separately and then against each other. An inferential analysis approach was used to compare the data between the groups. Creswell (2012) described this analysis as the most appropriate when comparing groups with two or more variables.

The researcher used the data and inferential analysis to test each of the hypotheses presented in Chapter 1. A two-sample assuming equal variances t-test was used to determine what differences existed between the means of the treatment and control groups. According to Salkind (2018), this type of test is most appropriate when a researcher wishes to examine differences between groups where the same participants are used for the pre- and post-test. An analysis of variance test was also considered for comparing the two groups. However, Creswell (2012) described this method as appropriate when dealing with three or more data groups.

Because this study only has two data groups, it was not chosen as the test for statistical significance.

Chapter Summary

Chapter 3 discussed the methodology for this quantitative, quasi-experimental study. The research method, design appropriateness, and rationale for this research were also explained. Other possible methods and designs were compared to show why the researcher chose the approaches he did. Next, population, sampling, instrumentation, and data collection procedures were described. Further, internal and external validity was discussed, with threats in each category analyzed against this study. Data analysis was also covered at a high level, with a two-sample assuming equal variances t-test chosen for the statistical comparison of the pre-and post-test data. This test allowed the researcher to compare the change between the data sets to answer the research questions best.

In Chapter 4, the data collected during the research will be discussed. The data were analyzed using pre-and post-test surveys, and statistical methods were used to find correlations between the treatment and control groups. Each hypothesis was tested to determine what if any, changes occurred.

CHAPTER 4: RESULTS

This chapter provides a detailed analysis of the data obtained during this study. This study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite Internet upon rural American customers. First, the pilot study results are reviewed to show any changes the researcher made to the pre-and post-test survey questions or instrumentation. Second, the data collection process is explained in detail for pre-and post-test, focusing on omitted data. Next, the pre-and post-test data, including the treatment and control groups' responses, are presented and analyzed using a two-sample assuming equal variances t-test to find potential statistical significance. Lastly, external and internal validity concerns are addressed. Chapter 5 will show the conclusions on each research question and recommendations made based on the data analyzed in Chapter 4.

Pilot Study

The pilot study was conducted using the same questions used for the pre-test survey but with the addition of four questions (Appendix C) at the end of the survey. The researcher chose three Facebook groups in Alabama, Wyoming, and Wisconsin to advertise the survey. The additional questions were not advertised, as the data collected was included in the pre-test results. The researcher did not want to force a change in opinion for those completing the survey. Seventeen responses were received within eight hours of the advertisement on October 25, 2021, and the goal of 15 responses set by the researcher was quickly met. Two respondents answered that they were either under 18 or had not pre-ordered Starlink; therefore, their results were omitted. Additionally, the pilot study questions were not required, and only nine participants chose to answer them.

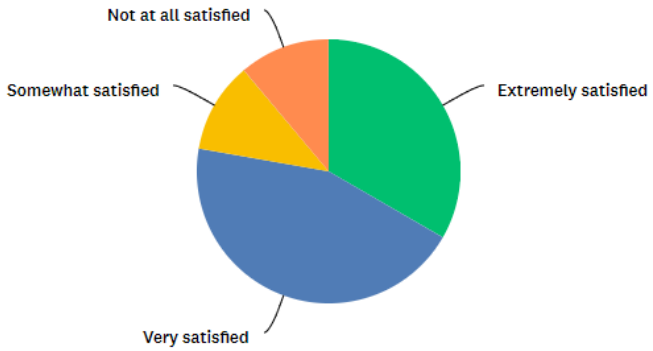
The first question asked how satisfied the participants were with the look and feel of the survey. Responses ranged from extremely satisfied to not at all satisfied; 77.77% of the participants indicated that they were very or extremely satisfied with the look and feel of the survey. The answers to this question are shown in Figure 15.

Figure 15

Pilot Study Question 16

How satisfied are you with the look and feel of this survey??

Answered: 9 Skipped: 8



ANSWER CHOICES	RESPONSES	
Extremely satisfied	33.33%	3
Very satisfied	44.44%	4
Somewhat satisfied	11.11%	1
Not so satisfied	0.00%	0
Not at all satisfied	11.11%	1
TOTAL		9

The next question was opened-ended, asking the participant what they liked about the survey. Although responses differed, most mentioned the accessible format and easy-to-answer questions. The results are listed below in Table 3.

Table 3

Pilot Study Question 17

#	RESPONSES	DATE
1	Simplicity	10/26/2021 4:16 PM
2	Facebook group	10/26/2021 4:10 PM
3	Nothing	10/26/2021 4:09 PM
4	Easy to answer questions	10/26/2021 3:54 PM
5	Ease of question and response process.	10/26/2021 3:48 PM
6	Easy format	10/26/2021 3:31 PM
7	It was quick and straight forward	10/26/2021 3:24 PM
8	Nothing	10/26/2021 3:01 PM
9	Easy	10/26/2021 10:26 AM

The next question asked each participant what they disliked about the survey. The majority of the respondents answered either not sure or nothing. Table 4 shows these results.

Table 3

Pilot Study Question 18

#	RESPONSES	DATE
1	Not sure	10/26/2021 4:16 PM
2	Do not ask country. My zip code is from Chile, not USA	10/26/2021 4:10 PM
3	It's a scam	10/26/2021 4:09 PM
4	N\A	10/26/2021 3:54 PM
5	Nothing	10/26/2021 3:48 PM
6	Some questions like this one don't pertain to topic	10/26/2021 3:31 PM
7	Nothing	10/26/2021 3:24 PM
8	Nothing	10/26/2021 3:01 PM
9	Nothing	10/26/2021 10:26 AM

The last question was again open-ended, asking each participant if they had any additional comments for the researcher. Eight participants responded, with 37.5% of them answering none. Table 5 shows this data.

Table 5

Pilot Study Question 19

#	RESPONSES	DATE
1	Find out when I might get service	10/26/2021 4:16 PM
2	You're an idiot. Let's go Brandon	10/26/2021 4:09 PM
3	None	10/26/2021 3:54 PM
4	Best wishes for your doctorate. I completed mine in a different subject several years ago. It's an exhausting, rigorous, but rewarding process!	10/26/2021 3:48 PM
5	Nope	10/26/2021 3:31 PM
6	None	10/26/2021 3:24 PM
7	How does this survey provide any useful data	10/26/2021 3:01 PM
8	Test	10/26/2021 10:26 AM

Because the pilot study results were primarily positive, with no changes requested, the researcher did not change the questions, format, or instrumentation used for the pre-and post-test surveys.

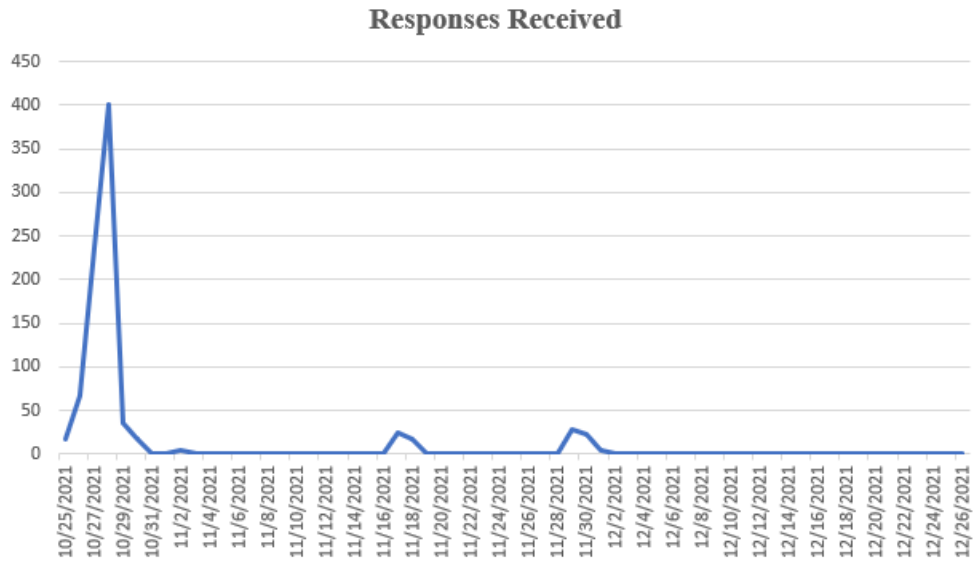
Pre-Test Data Collection Process

The pre-test survey was launched on October 26, 2021, using a surveymonkey.com public URL. As mentioned in Chapter 3, the researcher had joined Facebook groups created for rural dwellers before this date to advertise the survey. The researcher randomly chose ten groups to post the advertisement on the first day. By the end of the day, 65 responses had been received. Facebook advertisement continued on October 27, 2021, with five groups posting to gather participants. An additional 235 responses were received by the end of the second day, which significantly exceeded the researcher's expectations. This process was repeated until November 1, 2021, when Facebook suspended the researcher's account due to multiple reports to group administrators about the account being SPAM or false advertising. Even though administrators of the groups had approved, these reports of SPAM or false advertising to Facebook were an individual choice and out of the researcher's control. By this time, including the pilot survey, 770 responses had been received within seven days of the survey launch. On November 4, 2021, the researcher's

account was reinstated after an appeal was made; however, the permission to post to groups was not granted until November 10, 2021. Therefore, the researcher continued advertising the pre-test survey on November 10, 2021, at a rate of five different groups daily until groups were completed. This slower pace of advertisement was successful, as the account was not suspended again for the remainder of the 60-day survey period. The survey URL was closed on December 26, 2021, with 883 responses obtained, including the pilot. Figure 16 shows the responses received by date.

Figure 16

Pre-Test Response Count



Pre-Test Data Analysis

Of the 883 responses received over the 60-day timeframe, 679 (76.89%) were completed, meaning the participants answered all the questions on the survey. Questions 1 and 2 were qualifying, with a response of no disqualifying the participant immediately. Question 1 was answered “yes” by 100% of respondents, indicating they were of legal age. The IRB had only approved this research for those over 18. Question 2 asked if participants had pre-ordered but not

yet installed Starlink. This question ensured that the proper treatment and control groups were created, allowing for a detailed comparison with the post-test data. Eighty-one participants answered no to this question and were excluded from the survey. In addition, participants whose zip code was found to be located outside the United States were also omitted. The geography feature within Microsoft Excel was used first, with the researcher manually performing additional validation using the United States Postal Service zip code lookup tool. Further filtering was performed to exclude participants who incorrectly answered the questions, such as those who put a home address in place of the email address and those who provided four-digit zip codes instead of the required five. Finally, 630 participants were included in the pre-test data set.

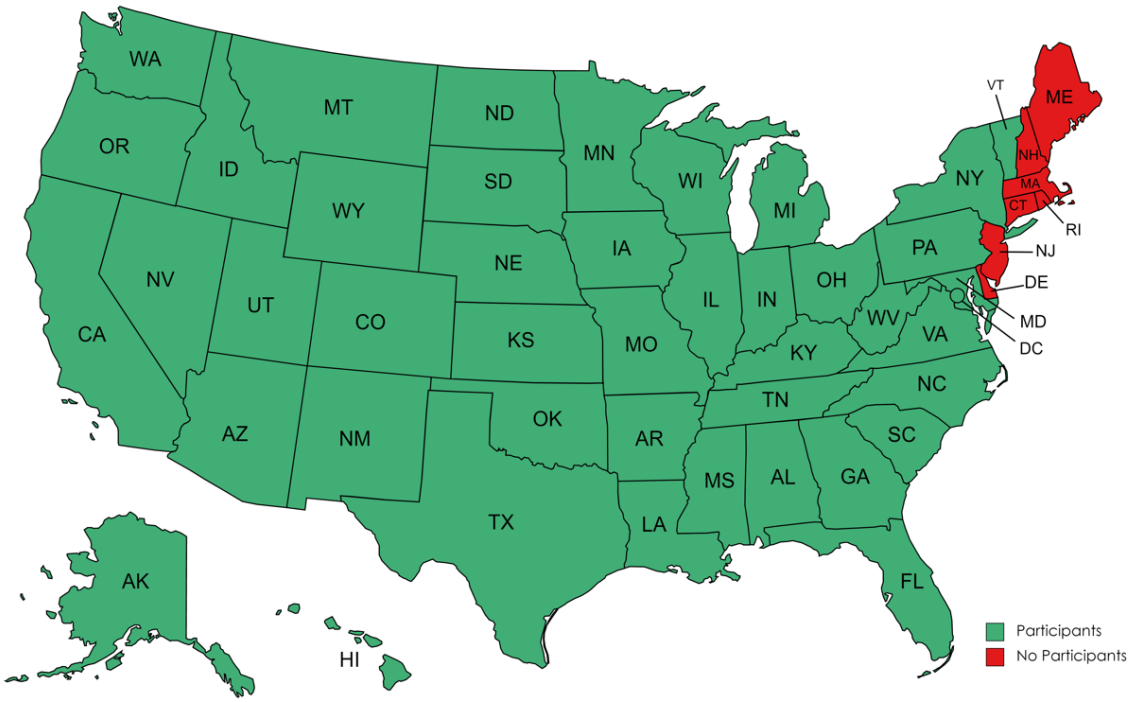
Location

This study focused on rural areas with a low population density where Starlink's competitors' technologies, such as 5G and other terrestrial broadband products, are unavailable (Musk, 2020). To limit non-rural area participation in the United States, the researcher targeted specific areas of each state with a population of less than 50,000. Of the 630 participants, 309 met the United States Census Bureau's (2019) definition of people residing in a rural location. The population average of these participants was 11,238. The remaining 321 participants had an average population of 1,100,391. The overall average was 504,730. Numerous high-density urban zip codes in New York City and Los Angeles led to a higher-than-targeted population.

The pre-test did not meet the researcher's goal of having at least one participant per state. Each state had a minimum of one participant except for Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, and Rhode Island. Figure 17 is a visual representation of the participants' location.

Figure 17

Pre-Test State Participation



Note: Created using www.mapchart.net. Reprinted with permission.

Household Size and High-Speed Internet Access

Pre-test survey question five asked for the number of people living in each participant's household. The United States Census Bureau (2020) reports an average of 2.60 people per household in the United States. The average for the 630 participants in the pre-test was 3.43 people per household, representing a 31.92% increase compared to the United States Census Bureau statistic. With 500,000 pre-orders for Starlink, if the alternative hypotheses were incorrect and statistical significance was proven, the risks may affect over 1,715,000 people.

Questions six, seven, and eight focused on whether the participant's households had high-speed internet access and if they expected their internet usage to increase once Starlink was

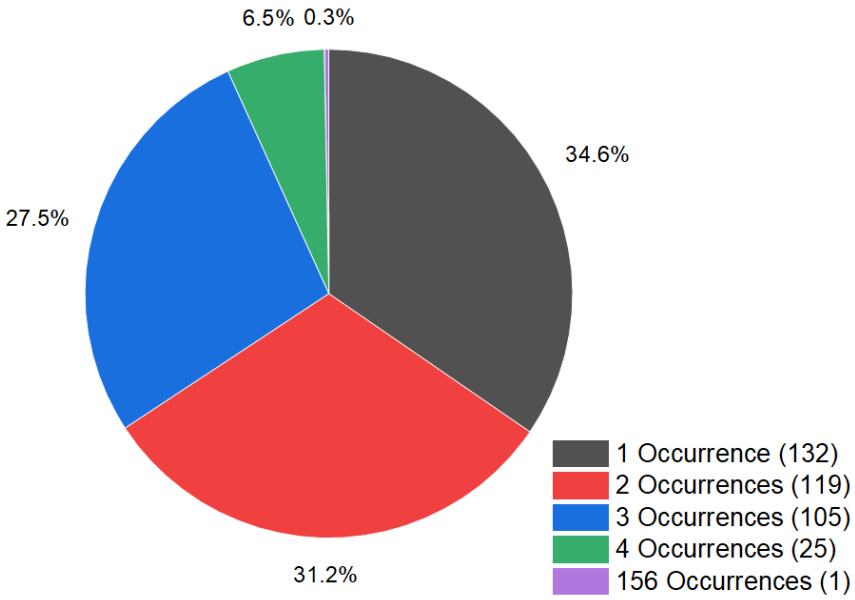
installed. Of the 630 participants, 516 (81.90%) answered that they currently had high-speed internet access, defined by the Federal Communications Commission (2020a) as at least 25 Mbps for downloads and 5 Mbps for uploads. One hundred (15.87%) participants answered no. Fourteen (2.22%) participants said they did not know. Of the 516 who answered yes to question six, 133 (25.77%), 227 (53.68%), and 106 (20.54%) answered that they had had access for less than a year, less than two years, and two years or more, respectively. When asked whether they expected an increase in their internet usage following the installation of Starlink, 533 (84.60 %) participants answered yes, 42 (6.66%) answered no, and the remaining 55 (8.73%) answered that no change was expected.

Research Question 1

Research question 1 seeks to understand if the occurrences of identity theft changed for end-users of Starlink in rural locations in the United States. Appendix A shows survey questions nine and ten related to identity theft. Of the 630 participants who answered the pre-test survey, 382 (60.63%) answered that they had experienced an incident of identity theft within the 24 months prior. Of these participants who answered yes, 105 (27.48%) indicated that a single incident had occurred; 132 (34.55%) said they had experienced two incidents, while 119 (31.15%) said they had experienced three. Twenty-five (6.54%) participants experienced four incidents of identity theft, and one person (.026%) indicated that they noticed 156 occurrences. Figure 18 shows the percentages of each occurrence for the 382 participants who answered yes to survey question nine.

Figure 18

Identity Theft Occurrences and Percentage of Total

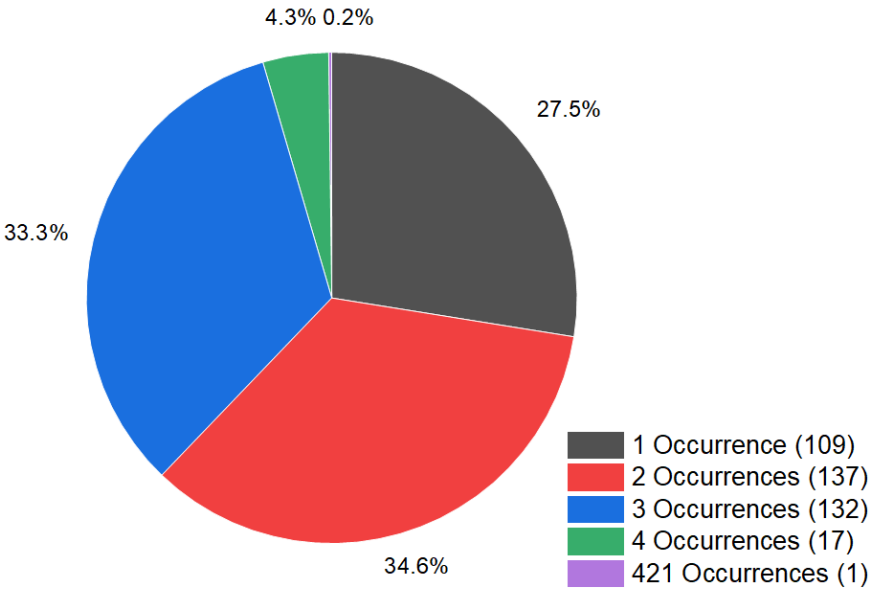


Research Question 2

Research question 2 seeks to understand if the occurrences of personal data breaches changed for end-users of Starlink in rural locations in the United States. As shown in Appendix A, survey questions number 11 and 12 were asked of each participant. Of the 630 participants who answered the pre-test survey, 396 (62.85%) answered that they had experienced an incident of a personal data breach within the 24 months prior. Of these participants who answered yes, 109 (27.59%) indicated that a single incident was observed; 137 (34.68%) experienced two incidents, while 132 (33.42%) experienced three. Seventeen (4.30%) participants experienced four personal data breach incidents, and one participant (.025%) indicated they noticed 420 occurrences. Figure 19 shows the percentages of each occurrence for the 396 participants who answered yes to survey question 11.

Figure 19

Personal Data Breaches Occurrences and Percentage of Total

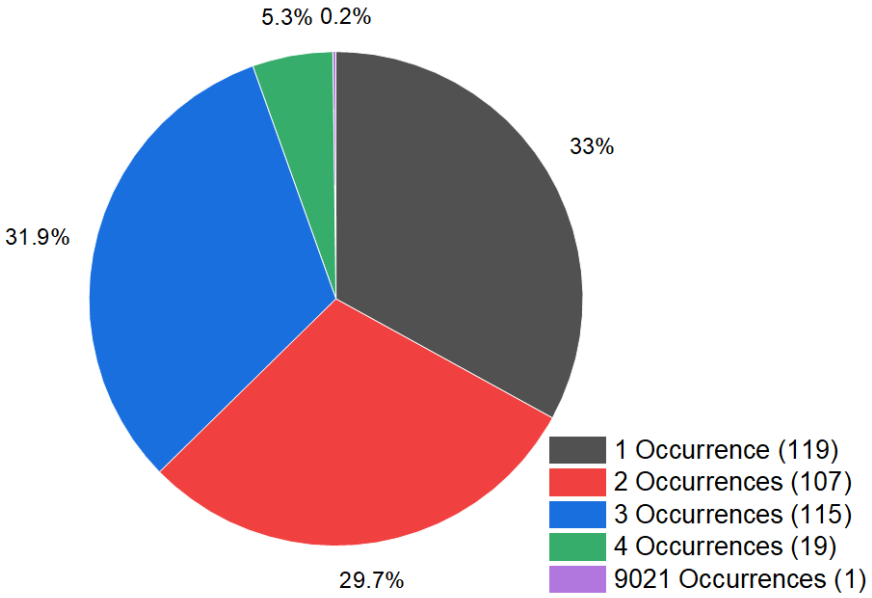


Research Question 3

Research question 3 seeks to understand if the occurrences of reputational harm changed for end-users of Starlink in rural locations in the United States. As shown in Appendix A, survey questions numbers 13 and 14 were asked of each participant. Of the 630 participants who answered the pre-test survey, 361 (57.30%) answered that they had experienced reputational harm in the 24 months prior. Of these participants who answered yes, 119 (32.96%) indicated that a single incident had occurred; 107 (29.63%) stated that they had experienced two incidents, while 115 (31.85%) participants stated that they had experienced three incidents. Nineteen (5.26%) participants experienced four incidents of reputational harm, while one participant (.025%) indicated that they observed 982 occurrences. Figure 20 shows the percentages of each occurrence for the 361 participants who answered yes to survey question 13.

Figure 20

Reputational Harm Occurrences and Percentage of Total

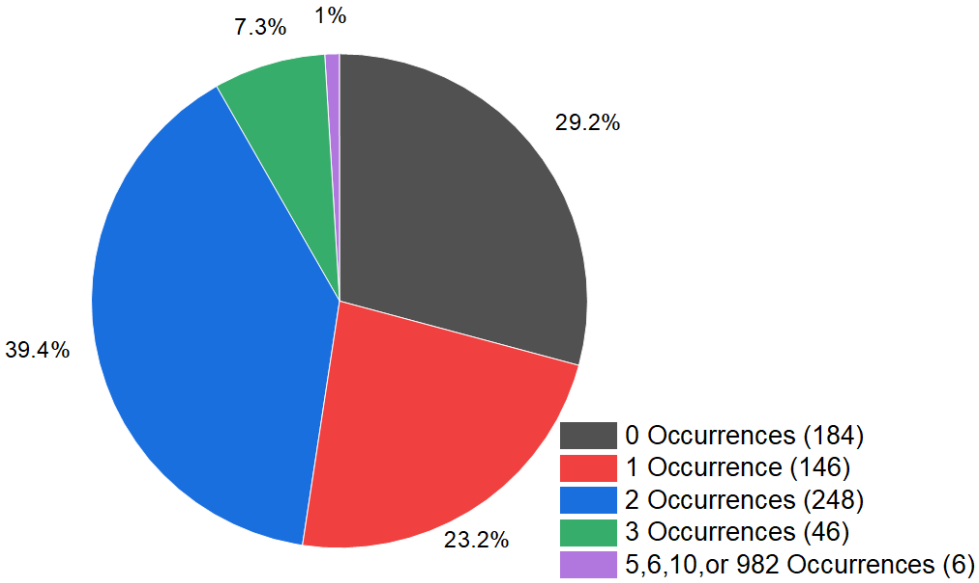


Research Question 4

Research question 4 seeks to understand if the occurrences of malware and viruses will change for end-users of Starlink in rural locations in the United States. As shown in Appendix A, survey question 15 was asked of each participant. From the 630 participants who answered the pre-test survey, 184 (29.20%) answered that they had experienced no malware or viruses on endpoints in their households in the 24 months prior. One hundred and forty-six (23.17%) indicated a single incident; 248 (39.36%) indicated three incidents, while 46 (7.30%) participants indicated four incidents. Six participants indicated more than four, with five, six, ten, ten, and 982 representing .16% of each. Figure 21 shows the percentages of each occurrence for the 630 total participants.

Figure 21

Malware and Viruses Occurrences and Percentage of Total



Post-Test Data Collection Process

The post-test survey was launched on June 21, 2022, using the public URL of surveymonkey.com. The duration between the commencement of the pre-and post-test was 238 days. The researcher chose this duration to allow ample time for treatment to occur. As previously noted, the treatment of the installation and use of Starlink was not a controllable, independent variable.

The researcher collected the participants' email addresses as part of the pre-test, as shown in question four in Appendix B. From the researchers' academic email account, 630 valid participants from the pre-test were contacted via email on June 21, 2022. For privacy, recipients were blind carbon copied. Figure 22 shows the message the researcher sent.

Figure 22

Post-Test Survey Launch E-Mail

From: Christopher Gerber
Sent: Tuesday, June 21, 2022 12:09 PM
Subject: Starlink Cybersecurity Risk (Post-Survey)

Thank you so much for your participation in my research regarding cybersecurity concerns with Starlink! As promised, the post-test survey is live and ready for your input:

https://www.surveymonkey.com/r/LXZ3HGJ

This is a vital part of the research, and I hope you will take the time to fill it out. Once all responses are collected, I will draw the winners for the $50 gift cards as promised and deliver them electronically.

Thank you again for your help in data collection as I pursue my doctoral degree.

Chris Gerber
Student, DSc, Cybersecurity
Capitol Technology University

The researcher noted that of the 630 recipients, 510 were returned as invalid by the destination email server, with the majority being rejected from gmail.com. A subsequent post-survey reminder email, sent to the same recipients on June 26, 2022, yielded the same results. The researcher noted this incident for further investigation and moved forward with the advertisement for the post-survey.

By the end of the day on June 21, 2022, 46 responses had been received. On June 22, 2022, the researcher posted the following on the same rural Facebook groups previously joined prior to the pre-test launch:

> *My name is Chris Gerber, and I am continuing research on Starlink as part of a doctor of science program in cybersecurity. If you participated in the first part of my survey posted here six months ago, the post-survey is live and can be accessed here:*
>
> *https://www.surveymonkey.com/r/LXZ3HGJ*
>
> *Once all responses are collected, I will draw the winners for the $50 gift cards as promised and deliver them electronically. Thanks in advance!*

June 22, 2022, yielded another 36 responses; 26 were received on June 23, 2022. The researcher sent a reminder email to participants whose email addresses had not returned as invalid on June 21, 2022. Figure 23 shows this communication.

Figure 11

Post-Survey Reminder Email

From: Christopher Gerber
Sent: Sunday, June 26, 2022 8:28 AM
Subject: RE: Starlink Cybersecurity Risk (Post-Survey)

If you have completed the post-survey, thank you! Your feedback is greatly appreciated.

For those that have not, there is still time! Please use the link below to complete the second part of this study:

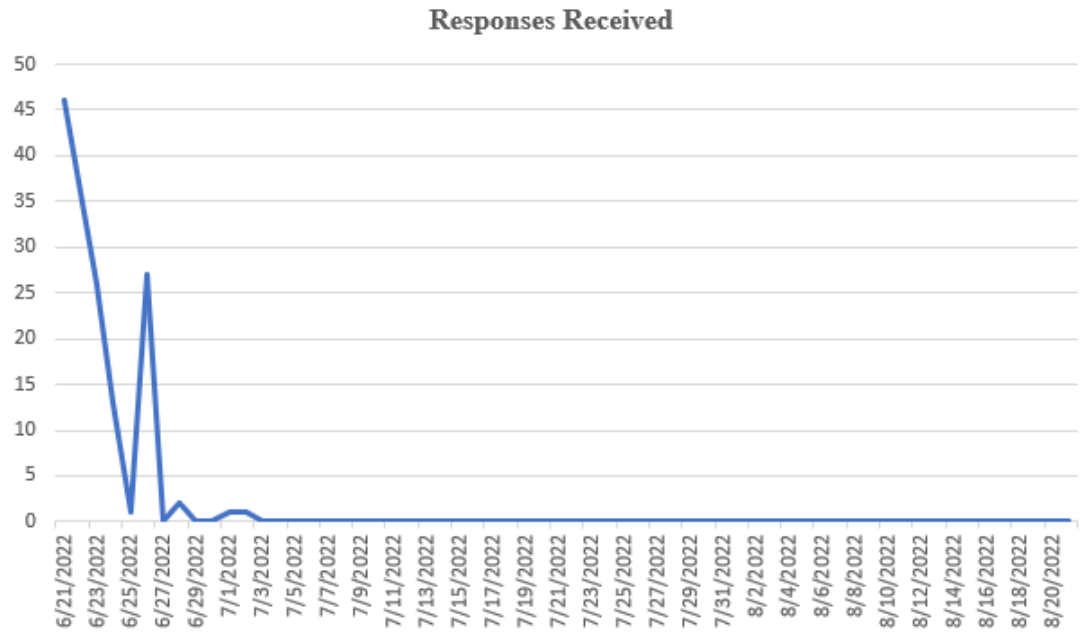
https://www.surveymonkey.com/r/LXZ3HGJ

Chris Gerber
Student, DSc, Cybersecurity
Capitol Technology University

Responses continued to be received, with a sharp drop-off observed after June 26, 2022. The survey URL was closed on August 21, 2022, with 153 responses obtained in total. Figure 24 shows the responses received by date.

Figure 24

Post-Test Response Count



Post-Test Data Analysis

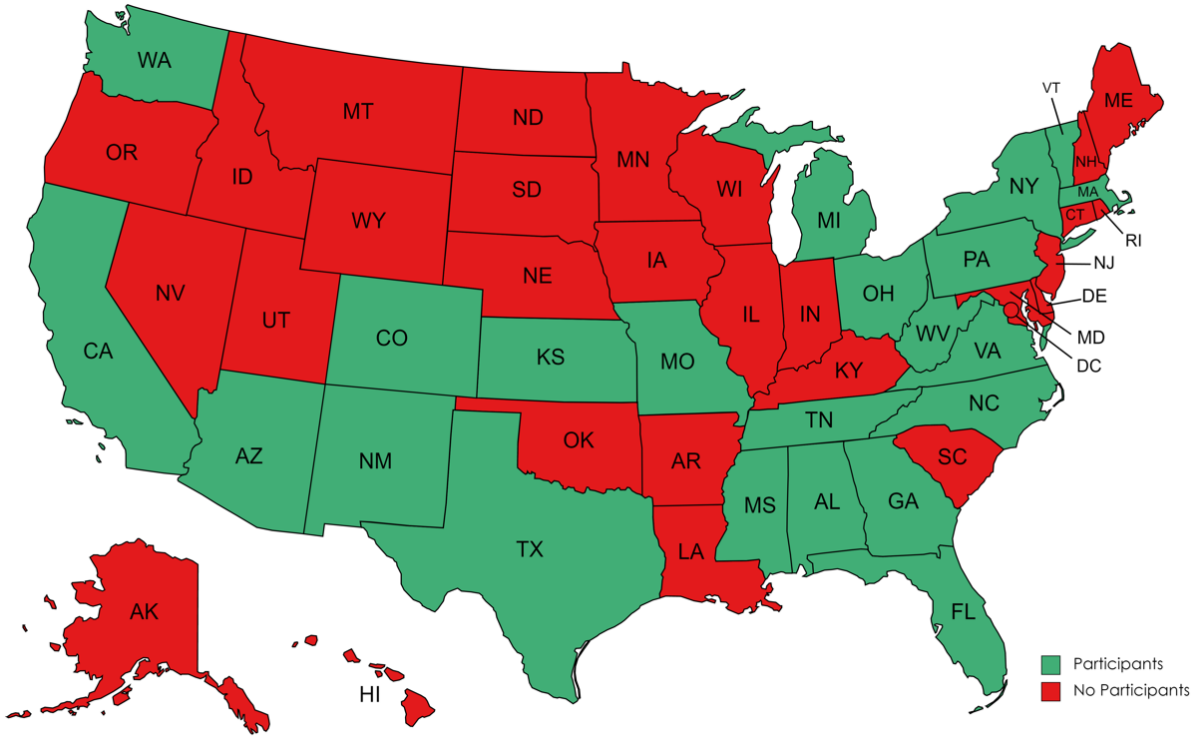
Of the 153 responses received over the 60 days, 118 (77.12%) were completed, meaning they answered all of the questions on the survey shown in Appendix C. As with the pre-test, question one was qualifying, with a response of no disqualifying the participant immediately. A 100% yes response was observed for Question 1, indicating that participants were of legal age. Questions two and three asked for the participant's email address and zip code. These two questions enabled the researcher to validate the participants by comparing the data to the pre-survey. Of the 118 participants who completed the survey, six provided zip codes outside the United States. These participants' responses were excluded, leaving 112 participants. To filter further, only those who matched email addresses and zip codes were excluded, leaving 47 participants. For these 47 participants, no change in zip code was observed between the pre-and post-test data.

Location

This study focused on rural areas with a low population density. To limit non-rural area participation in the United States, the researcher targeted specific areas within each state with the pre-test with populations of less than 50,000. Of the 47 participants, 45 (95.74%) met the United States Census Bureau's (2019) definition of residing in a rural location. The population average of these participants was 9,926.61. The remaining two participants had an average population of 66,436.50. The overall average was 12,657.04. The post-test did not meet the researcher's goal of having at least one participant per state. Figure 25 is a visual representation of the participants' location.

Figure 25

Post-Test State Participation



Note: Created using www.mapchart.net. Reprinted with permission.

Household Size & Starlink Treatment

Post-test survey question four asked about the number of people living in each participant's household. The average for the 45 valid participants was 3.00 people per household, representing a 13.33% increase compared to the statistical average of 2.60 (United States Census Bureau, 2020). This question was asked to determine whether the household size for included participants changed over the six months between the pre-and post-surveys. No change was observed between the pre-and post-test participants.

Post-test survey question five asked whether Starlink had been installed since the pre-test, with question six asking for the approximate installation date. The treatment and control groups for this study were determined using question four. Of the 45 participants, 29 (75.89%) received the treatment of installing and using Starlink, while 17 (24.10%) did not. Each participant was assigned an alphanumeric identifier to track their movement throughout the study. Control group participants were assigned an 0XX-C and treatment participants a 00XX-T, with X representing a number. For the 29 participants who received the treatment of Starlink, the average treatment duration was 87.90 days. Participants 002-T and 027-T had the most prolonged duration, with 117 days, while 005-T had installed and started the treatment of Starlink one day before answering the post-test survey. As described previously, the treatment variables, including length, were out of the researcher's control.

Dependent upon their response to question five, the participants were directed to either the treatment or control group questions. Both sets of questions were identical, except for the wording “treatment of Starlink” or “in the past six months” and two high-speed internet questions for the control group, as seen in Appendix C. All questions were similar to the pre-test to answer the research questions best.

High-Speed Internet Access

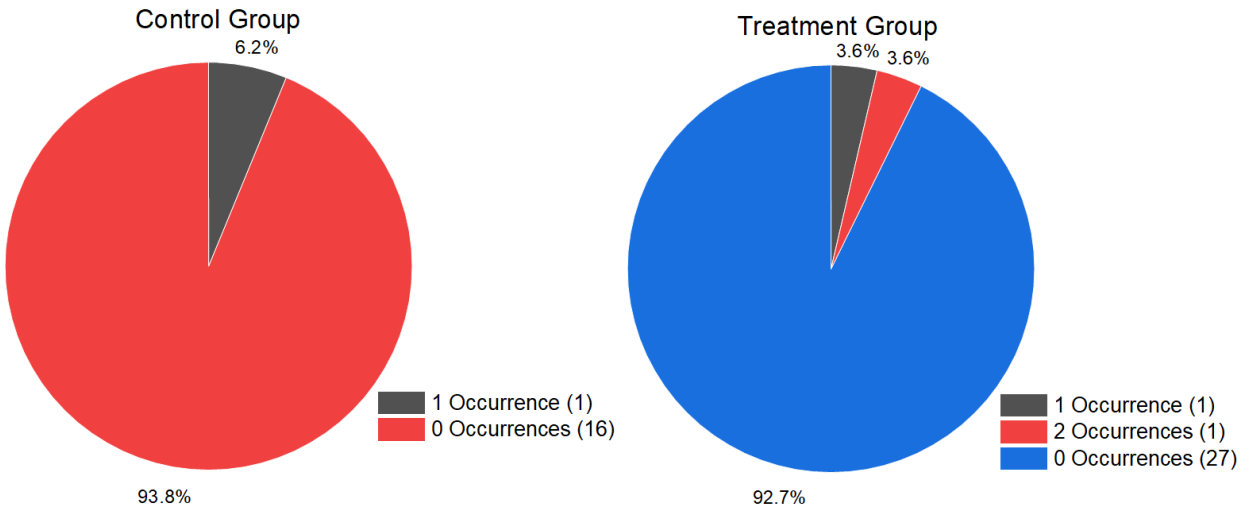
Post-test survey questions 14 and 15 focused on whether the participant's household had high-speed internet access and for what length. Four (23.52%) of the 17 control group participants answered that they currently had high-speed internet access. Eleven (64.70%) participants answered no, while two (11.76%) answered unknown. Of the four who answered yes to question 14, one (25.00%) answered that they had had access for less than a year; one (25.00%) answered that they had had access for less than two years, and one (25.00%) stated that they had had high-speed internet for two years or more. The last participant chose not to answer question 15.

Research Question 1

Research question 1 seeks to understand whether the occurrences of identity theft changed for end-users of Starlink. Both the control and treatment groups were reviewed. As shown in Appendix C, survey questions nine, ten, sixteen, and seventeen were asked of each participant. Of the 17 control group participants, one (6.25%) answered that they had experienced an identity theft incident six months prior. This participant only experienced one event. The remaining 16 (94.11%) answered no. Of the 29 participants in the treatment group, two (6.89%) indicated that they had experienced an identity theft incident since their installation and use of Starlink. The remaining 26 (89.65%) experienced no incidents. One of these participants experienced two events, while the other experienced one. Figure 26 shows the percentages of each occurrence and count for each group.

Figure 26

Identity Theft Occurrences and Percentage of Total for Groups

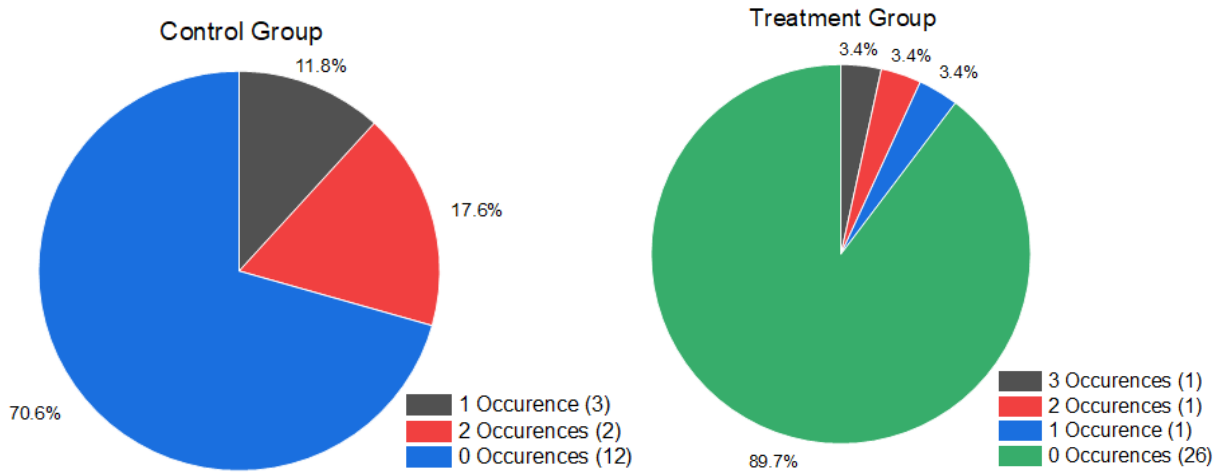


Research Question 2

Research question 2 seeks to understand whether personal data breach occurrences changed for Starlink's end-users. As shown in Appendix B, survey questions nine, 10, 18, and 19 were asked of each participant. Of the 17 control group participants, five (29.41%) answered that they had experienced a personal data breach within the six months prior, while the remaining 12 (70.58%) had no incidents. Three (17.64%) participants experienced one event, while the remaining two (11.76%) experienced two. Of the 29 participants in the treatment group, three (10.34%) experienced a breach since installing and using Starlink. The remaining 26 (89.65%) experienced no incidents. One of these participants experienced three events, one experienced two, and the last experienced one, representing 3.44% each. Figure 27 shows the percentages of each occurrence and count for each group.

Figure 27

Data Breach Occurrences and Percentage of Total for Groups

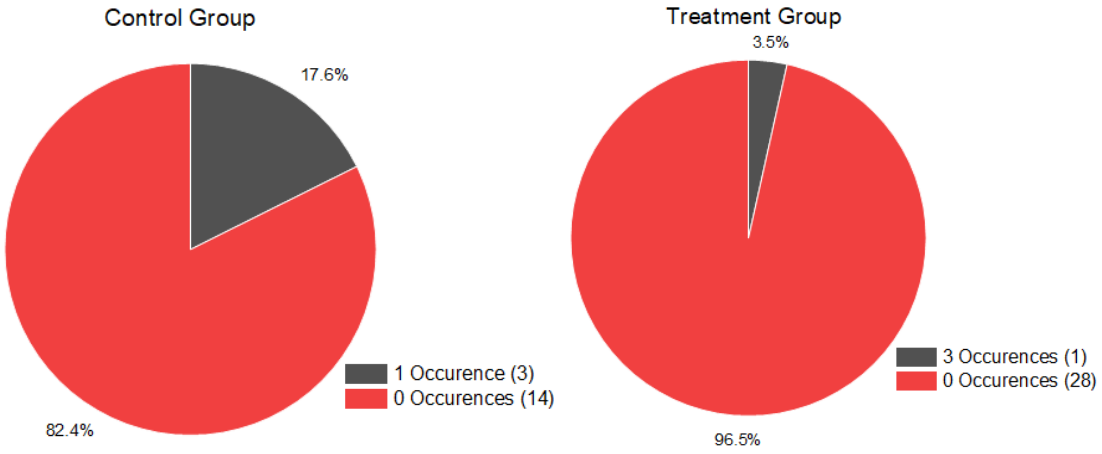


Research Question 3

Research question 3 seeks to understand if the occurrences of reputational harm changed for end-users of Starlink. As shown in Appendix C, survey questions numbers 11, 12, 20, and 21 were asked of each participant. Of the 17 control group participants, three (17.64%) answered that they had experienced reputational harm within the six months prior, while the remaining 14 (82.35%) experienced no incidents. Three (17.64%) participants experienced a single event. The treatment group of 29 had one (3.44%) participant experiencing reputational harm since their installation and use of Starlink. The remaining 28 (96.55%) experienced no incidents. The participant experienced three events, representing 3.44% of the total. Figure 28 shows the percentages of each occurrence and count for each group.

Figure 28

Reputational Harm Occurrences and Percentage of Total for Groups

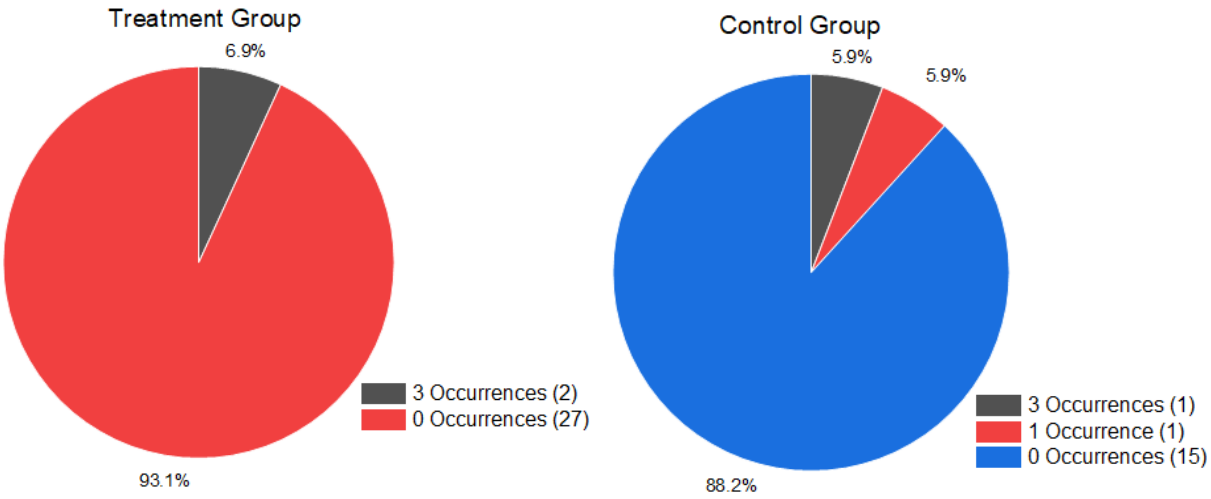


Research Question 4

Research question 4 seeks to understand if the occurrences of malware and viruses will change for end-users of Starlink. As shown in Appendix C, survey questions 13 and 23 were asked of each participant. Of the 17 control group participants, two (11.76%) answered that they had experienced an incidence of malware or viruses in the six months prior. The remaining 15 (88.23%) experienced no incidents. One (5.88%) participant experienced a single event; the other experienced three (5.88%) events. In the treatment group of 29, two (6.89%) participants had experienced malware or viruses since they installed and used Starlink. These participants experienced three events each, representing 6.89% of the total, and the remaining 27 (93.10%) experienced no incidents. Figure 29 shows the percentages of each occurrence and count for each group.

Figure 29

Malware and Virus Occurrences and Percentage of Total for Groups



Pre and Post-Test Data Comparison

To compare the results from the control and treatment groups, the researcher determined the average number of events for each of the four research questions. To determine this figure, the number of unique occurrences was divided by the number of participants for each group. The researcher defined this as the occurrence rate. As previously discussed, the treatment length average for those who installed and used Starlink was 87.90 days. The length for the control group was pre-determined as 180 days based on the survey questions in Appendix C. The disparity of 92.10 days caused the researcher to determine how to level each group to answer best the hypotheses posed.

Vanderweele and Arah (2011) defined this type of data disparity as an unmeasured confounder. They determined that it must be accounted for to limit bias when comparing two groups in a study. They also gave several examples, with the outcome of bias formulas to ensure a constant prevalence between each group. Chiba (2012) also proposed a similar method for

unmeasured confounding correction by finding the average of the observed uneven variables and adjusting based on the difference found.

The researcher performed a similar mathematical exercise on the treatment group to remove the 92.10-day difference in treatment days. The average of each occurrence observed was divided by the average treatment length of 87.90 to determine the per-day average. This figure was multiplied by 92.65 and added back to each occurrence average. The formula used is shown below in Figure 30.

Figure 30

Unmeasured Confounder Formula

$$x \div y = z$$
$$z \times 92.65 = w$$
$$w + x = \text{Normalized Occurrence Rate}$$

$$x = \text{Average Occurrence Rate}$$
$$y = \text{Treatment Length}$$

This formula was performed on each of the four occurrence rates prior to data comparison with the control group.

Research Questions

The occurrence rates for each research question for the 47 valid participants are shown in Table 6. These figures are based on the pre-test data set.

Table 4

Pre-Test Occurrence Rates

Research Question	Occurrence Rate (Per Participant)
1-Identity Theft	0.2
2-Data Breach	0.11
3-Reputational Harm	0.17
4-Malware and Viruses	0.46

The occurrence rates for the control group, those who were not exposed to the treatment of Starlink, are shown in Table 7. These figures are based on the post-test data set.

Table 5

Post-Test Occurrence Rates (Control Group)

Research Question	Occurrence Rate (Per Participant)
1-Identity Theft	0.21
2-Data Breach	0.42
3-Reputational Harm	0.22
4-Malware and Viruses	0.21

The occurrence rates of each event for the treatment group exposed to Starlink are shown in Table 8. These figures are based on the post-test data set.

Table 6

Post-Test Occurrence Rates (Treatment Group)

Research Question	Occurrence Rate (Per Participant)
1-Identity Theft	0.06
2-Data Breach	0.44
3-Reputational Harm	0.18
4-Malware and Viruses	0.24

The researcher compared the pre-and post-test occurrence rates to determine if a change was observed between the treatment and control groups. Tables 9 and 10 show the differences observed for both groups.

Table 7

Control Group Occurrence Rate Differences

Research Question	Pre-Test Occurrence Rate	Control	Difference
1-Identity Theft	0.2	0.06	-0.14
2-Data Breach	0.11	0.44	0.33
3-Reputational Harm	0.17	0.18	0.01
4-Malware and Viruses	0.46	0.24	-0.22

Table 8

Treatment Group Occurrence Rate Differences

Research Question	Pre-Test Occurrence Rate	Treatment	Difference
1-Identity Theft	0.2	0.21	0.01
2-Data Breach	0.11	0.42	0.31
3-Reputational Harm	0.17	0.22	0.05
4-Malware and Viruses	0.46	0.21	-0.25

Table 11 shows the observed change and percentage difference per occurrence, comparing the treatment and control groups.

Table 11

Observed Change Between Treatment and Control Groups

Research Question	Observed Change (Per Occurrence)	Percentage
1-Identity Theft	0.15	107.14
2-Data Breach	-0.02	-4.55
3-Reputational Harm	0.04	22.22
4-Malware and Viruses	-0.03	-12.5

T-Test

Creswell (2012) explained that proving the null hypothesis false is critical in research. In addition to the mathematical results, the appropriate statistical significance test must be performed on the data (Creswell, 2012). A two-sample assuming equal variances t-test was used to determine the differences between the treatment and control groups. The researcher chose the equal variable test because the differences observed between the pre-and post-test data are less than 4, and according to Creswell (2012), it is the standard method. The result of this test is known as the p-value. “A p value is the probability (p) that a result could have been produced by chance if the null hypothesis were true” (Creswell, 2012, p. 189). The formula used to conduct this test is shown in Figure 31.

Figure 31

Two-sample Assuming Equal Variances T-test

$$s_p = \sqrt{\frac{s_{X_1}^2 + s_{X_2}^2}{2}}.$$

where

$$t = \frac{\bar{X}_1 - \bar{X}_2}{s_p \sqrt{\frac{2}{n}}}$$

The researcher used Excel's statistical data analysis tool to compare the data sets for each hypothesis. A significance value of .05 was chosen, indicating a 5% chance of concluding that a difference exists when none exists. The researcher chose this level based on the small sample size in the study. Kim and Choi (2019) explained that the significance level must be set at a much lower value when the sample size is larger than the standard .05 or .01 measurements.

Research Question 1

An increase of .15 in identity theft occurrences per user was observed in the treatment group compared to the control group. Results of the t-test for each group are shown in Tables 12 and 13.

Table 12

Research Question 1 T-Test (Control Group)

Control Group		
	Pre-Test	*Post-Test*
Mean	0.117647059	0.058823529
Variance	0.235294118	0.058823529
Observations	17	17
Pooled Variance	0.147058824	
Hypothesized Mean Difference	0	
df	32	
t Stat	0.447213595	
P(T<=t) one-tail	0.328866686	
t Critical one-tail	1.693888748	
P(T<=t) two-tail	0.657733372	
t Critical two-tail	2.036933343	

Table 13

Research Question 1 T-Test (Treatment Group)

Treatment Group		
	Pre-Test	*Post-Test*
Mean	0.24137931	0.213173322
Variance	0.332512315	0.167487685
Observations	29	29
Pooled Variance	0.25	
Hypothesized Mean Difference	0	
df	56	
t Stat	0.214810409	
P(T<=t) one-tail	0.415347748	
t Critical one-tail	1.672522303	
P(T<=t) two-tail	0.830695496	
t Critical two-tail	2.003240719	

The p-value of the control group t-test was .65, which is not statistically significant when comparing the occurrence rate between the pre-and post-test. The p-value of the treatment t-test was .83, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test.

Research Question 2

A .02 decrease in the occurrences of data breaches, or -4.55% per user, was observed in the treatment group compared to the control group. Results of the t-test for each group are shown in Tables 14 and 15.

Table 14

Research Question 2 T-Test (Control Group)

Control Group		
	Pre-Test	*Post-Test*
Mean	0	0.411764706
Variance	0	0.507352941
Observations	17	17
Pooled Variance	0.253676471	
Hypothesized Mean Difference	0	
df	32	
t Stat	-2.38351829	
P(T<=t) one-tail	0.011625691	
t Critical one-tail	1.693888748	
P(T<=t) two-tail	0.023251382	
t Critical two-tail	2.036933343	

Table 15

Research Question 2 T-Test (Treatment Group)

Treatment Group		
	Pre-Test	*Post-Test*
Mean	0.172413793	0.426346644
Variance	0.290640394	0.455665025
Observations	29	29
Pooled Variance	0.373152709	
Hypothesized Mean Difference	0	
df	56	
t Stat	-1.58292227	
P(T<=t) one-tail	0.059535524	
t Critical one-tail	1.672522303	
P(T<=t) two-tail	0.119071049	
t Critical two-tail	2.003240719	

The p-value of the control group t-test was .02, which is statistically significant when comparing the occurrence rate of data breaches between the pre-and post-test. The p-value of the treatment t-test was .11, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test.

Research Question 3

An increase of .04 (22.22%) in the occurrence of reputational harm was observed per user in the treatment group compared to the control group. Results of the t-test for each group are shown in Tables 16 and 17.

Table 16

Research Question 3 T-Test (Control Group)

Control Group		
	Pre-Test	*Post-Test*
Mean	0.235294118	0.176470588
Variance	0.941176471	0.154411765
Observations	17	17
Pooled Variance	0.547794118	
Hypothesized Mean Difference	0	
df	32	
t Stat	0.231713779	
P(T<=t) one-tail	0.409117856	
t Critical one-tail	1.693888748	
P(T<=t) two-tail	0.818235713	
t Critical two-tail	2.036933343	

Table 17

Research Question 3 T-Test (Treatment Group)

Treatment Group		
	Pre-Test	*Post-Test*
Mean	0.137931034	0.213173322
Variance	0.266009852	0.310344828
Observations	29	29
Pooled Variance	0.28817734	
Hypothesized Mean Difference	0	
df	56	
t Stat	-0.53372319	
P(T<=t) one-tail	0.297822668	
t Critical one-tail	1.672522303	
P(T<=t) two-tail	0.595645336	
t Critical two-tail	2.003240719	

The p-value of the control group t-test was .81, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test. The p-value of the treatment t-test was .59, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test.

Research Question 4

A decrease of .03 (-12.5%) was observed in the occurrence of malware and viruses per user in the treatment group compared to the control group. Results of the t-test for each group are shown in Tables 18 and 19.

Table 18

Research Question 4 T-Test (Control Group)

Control Group

	Pre-Test	*Post-Test*
Mean	0.647058824	0.235294118
Variance	5.867647059	0.566176471
Observations	17	17
Pooled Variance	3.216911765	
Hypothesized Mean Difference	0	
df	32	
t Stat	0.669328021	
P(T<=t) one-tail	0.254043538	
t Critical one-tail	1.693888748	
P(T<=t) two-tail	0.508087076	
t Critical two-tail	2.036933343	

Table 19

Research Question 4 T-Test (Treatment Group)

Treatment Group

	Pre-Test	*Post-Test*
Mean	0.344827586	0.213173322
Variance	0.448275862	0.167487685
Observations	29	29
Pooled Variance	0.307881773	
Hypothesized Mean Difference	0	
df	56	
t Stat	0.903497473	
P(T<=t) one-tail	0.185066085	
t Critical one-tail	1.672522303	
P(T<=t) two-tail	0.37013217	
t Critical two-tail	2.003240719	

The p-value of the control group t-test was .50, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test. The p-value of the treatment t-test was .37, which is not statistically significant when comparing the occurrence rate between the pre-test and post-test.

Validity/Reliability

Of the 630 pre-test participants who completed the survey, only 49 were considered valid based on their responses to the post-survey, bringing the instrument's validity and reliability into question. The researcher first suspected that something had gone wrong when Google returned 510 of the post-survey email invitations shown in Figure 24, showing that they did not exist. To investigate, the researcher performed a Google.com search with the survey URL and Facebook advertisement data to determine if the survey was posted in other online locations. Nothing was found, meaning that a nefarious actor was attempting to skew results for result manipulation or

financial gain. Using each participant's email address and zip code allowed the researcher to gain confidence in the remaining 49 participants who provided accurate answers. Additionally, the pilot survey questions provided proper feedback for the researcher.

The researcher set a goal for a single participant per state; this goal was not met, with only 22 states in the final results. However, the goal of primarily rural area participation was met, with a population average of 12,657.04. In addition to what was described above in the pre-test, the roll-out schedule of Starlink affected participation. The researcher placed a pre-order and received an email From Starlink indicating delays:

> Thank you for being a supporter of Starlink! Over 14 million people have inquired about Starlink service in their area, and today, Starlink is available in over 20 countries (and counting). The Starlink team has been working hard to expand service and increase capacity while continuously improving quality of service. We will be able to accommodate more users per area as we increase the number of satellites in orbit. Silicon shortages over the last 6 months have slowed our expected production rate and impacted our ability to fulfill many Starlink orders this year. We apologize for the delay and are working hard across our engineering, supply chain, and production teams to improve and streamline our product and factory to increase our production rate. (personal communication, November 23, 2021)

Chapter Summary

Chapter 4 described the data retrieved from the pre-and post-tests. The control and treatment groups were presented, including the occurrence rates and percentage changes for the four research questions. The pilot study was also discussed, providing valuable feedback regarding the validity and reliability of the instrumentation. Other pertinent data, such as

location, household size, and previous access to high-speed internet, were reviewed in detail. The statistical relevance of the data for each research question was also presented using an equal variance t-test. Finally, the validity and reliability of the study were discussed. Chapter 5 will expand upon the data presented in Chapter 4 to draw the appropriate limitations, conclusions, and future research recommendations. It will use the theoretical risk framework with ISO 31000 as a guide.

CHAPTER 5: FINDINGS AND RECOMMENDATIONS

This quantitative, quasi-experimental, exploratory study's purpose was to determine the cybersecurity risks posed by Starlink LEO satellite internet to rural American customers. Chapter 5 contains the findings and recommendations for this study based on the data presented in Chapter 4. The limitations, interpretations, recommendations, and future research suggestions are covered. In addition, a final summary of each of the five chapters of this dissertation is provided.

The limitations section reviews how this study was impacted by sample size, event timing, and more factors. The findings section uses ISO 3100 as a guide for interpreting the research data. Recommendations are made to end-users, SpaceX, and academia using the data within this study. Future recommendations are also made for those who wish to further this research.

As discussed in Chapter 2, an extant gap in the literature exists for the end-user cybersecurity risks of Starlink usage. The researcher's original contribution to knowledge shows increased occurrence rates of identity theft and reputational harm for Starlink end-users compared to the control group. A decrease was observed in malware, viruses, and data breach risks.

Limitations

Chapter 1 described limitations with the participants understanding the definitions of cybersecurity risk. The researcher minimized this limitation by crafting survey questions with specific examples for each participant to consider before answering the question. This method educated the participants on the topic, even if they had previously had zero or limited exposure.

No negative feedback was received for the pilot study, allowing the researcher to move forward with the questions as written.

Willingness to disclose information was also identified as a potential limitation. The researcher only asked for email addresses and zip codes as part of the survey, so no personally identifiable information was collected. The researcher believes this allowed the participants to answer truthfully, although this cannot be proven. The researcher made every effort to market the post-test to the pre-test participants. Email and Facebook posts were created and sent to pre-test participants. In addition, reminders were also sent over the 60-day length of the post-survey. The data set was limited, with only 49 of the 100-participant goal of the researcher realized. The independent variable of treatment was another limitation that was not controllable. Therefore, the control and treatment groups were not equal in size, which was considered when determining which statistical relevance test to perform.

Findings and Interpretations

Chapter 4 displayed the pre-and post-test results and described the t-test performed to determine relevance. This section examines the data to answer the research questions and hypotheses. As discussed in previous chapters, the independent variable was Starlink installation and use, while the dependent variable was the occurrence rate of each research question. The differences between the control and treatment groups are reviewed to determine if Starlink use affected the occurrence rates.

Research Question 1

Research question 1 asked if the occurrence rate of identity theft will change for end-users of Starlink in rural locations in the United States. The data in Table 11 shows a .15 (107.14%) increase in the occurrence rates of identity theft for Starlink users compared to those

in the control group. This data alone is enough to reject the null hypothesis that the difference in the incidence of identity theft will not increase between the control group and those exposed to the treatment of Starlink. However, the results of the two-sample assuming equal variances t-test for the treatment group was .83, which was not statistically significant; therefore, the null hypothesis was accepted and the alternative hypothesis rejected.

Research Question 2

Research question 2 asked if the occurrences of a personal data breach will change for end-users of Starlink in rural locations in the United States. The data in Table 11 shows a -.02 (4.55%) decrease in the occurrence of a personal data breach for Starlink users compared to those in the control group. The null hypothesis is that the incidence of a personal data breach will not increase among those exposed to the treatment of Starlink compared to the control group. Although a decrease was observed, the t-test result for the treatment group data was .11, which was not statistically significant. Therefore, the null hypothesis was accepted, and the alternative hypothesis that occurrences will increase was rejected.

Research Question 3

The third research question asked if the occurrences of reputational harm will change for end-users of Starlink in rural locations in the United States. Table 11 shows a .04 (22.22%) increase in the incidence of reputational harm among Starlink users compared to those in the control group. This increase supports rejecting the null hypothesis that reputational harm occurrences will not increase among those exposed to the treatment of Starlink compared to the control group. However, the p-value of .59 indicates that the change was not statistically significant; therefore, the null hypothesis was accepted, and the alternate hypothesis was rejected.

Research Question 4

Research question 4 seeks to understand if the occurrences of malware and viruses will change for end-users of Starlink in rural locations in the United States. A -.03 (12.5%) decrease in the incidence of malware and viruses was observed among the treatment compared to the control groups. Although this change rejects the null hypothesis that malware and virus occurrences observed will not increase between the control group and those exposed to the treatment of Starlink, the p-value of .37 on the t-test does not support the significance of the change. Therefore, the null hypothesis that malware and virus occurrences observed will not increase among those exposed to the treatment of Starlink compared to the control group was accepted.

Framework Interpretation

As discussed in Chapter 1, the International Organization for Standardization (2018) lists five steps that must be performed continuously to identify and mitigate product risk. For the context of results interpretation, the researcher performed the third step in the process. This step states that stakeholders must be adequately educated on the product and understand all risks (International Organization for Standardization, 2018). Even without a statistically significant result, specific cybersecurity risk changes did occur that potentially may be used in further research and recommendations to Starlink and their current and future customers, who are key stakeholders.

Risk identification is essential to adequate education (International Organization for Standardization, 2018). The following factors must be considered when performing this function:

- tangible and intangible sources of risk;
- causes and events;

- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- time-related factors; and
- biases, assumptions, and beliefs of those involved. (International Organization for Standardization, 2018, p. 6)

Among these factors, potential sources of risk, threats, and opportunities were the primary focus of this study. The source of risk was shown to be the installation and use of the Starlink product. Using control and treatment groups allowed the researcher to compare the change in the value of the independent variable. The per-occurrence difference for each research question shows potential threats and opportunities for change, which is covered in the recommendations section of this chapter.

Recommendations

The researcher recommends that SpaceX reviews this data as a potential risk, threat, and opportunity for their Starlink product. Although focused on the United States rural areas, the data may easily be transferred to other customers in different locations globally. Opportunity exists for the development of methods to combat this risk. For example, new customers can be offered cybersecurity awareness training to protect themselves from identity theft, data breaches, reputational harm, malware, and viruses before use. Another method is to offer an inline security

product to protect Starlink users' internet traffic, if they choose, by scanning it for common threats and vulnerabilities and proactively preventing them.

Another potential risk for SpaceX to investigate, if they have not already done so, is the LEO-specific risks outlined in Chapter 2. There are multiple threats to the space, ground, and user segments, including software vulnerabilities, supply chain, eavesdropping, jamming, space debris, signal interference, and eavesdropping. The researcher recommends that SpaceX follows the ISO 31000 approach to these risks with the outcome of user and stakeholder education on their findings.

Recommendations for Future Research

While the results of this study did not show statistical significance between the control and treatment groups, changes did occur to the cybersecurity risk occurrence scores for specific research questions. Due to these changes and the data displayed in Chapter 2, there are multiple recommendations for future research. First, a qualitative study can be performed on privacy laws and regulations and how they relate to satellite internet access by country; the Chinese government's control over ISPs and their operations is an example described in Chapter 2.

Second, the effects of using high-speed internet on the cybersecurity risk of the end-users due to external factors must be studied. This study focused on the possibility of a risk increase but did not discuss factors such as education, location, race, gender, or other demographics that may contribute to a change. A country such as the United States, which has seen an increase in racial and ethnic diversity since 2010, will be a good candidate for this type of study (United States Census Bureau, 2022).

Third, the researcher recommends broadening this research to include a larger population sample to increase the data set. The research may also be ported to another form of emerging

Internet access to gain more convenience and relevant results. With an increased data set and possible statistical significance, the results may be applied to the cost-benefit analysis calculation to determine how the cybersecurity risk compares to the benefit of Internet access at an increased rate of speed for end-users.

Finally, a study can be conducted on the increased international regulation of the space industry, particularly over satellites in LEO that provide internet access. For example, the FCC serves as the approval authority in the United States for SpaceX to operate Starlink, with various entities providing similar functions in other countries (Federal Communications Commission, 2020a). Currently, the United Nations oversees five international treaties regarding space regulation through a specific committee (United Nations Committee on the Peaceful Uses of Outer Space, 2022). Detailed research can help determine if these treaties provide adequate coverage for the global industry and make recommendations for change.

Summary

This quantitative, quasi-experimental dissertation explored the problem of LEO internet changing the risk profile of internet-connected devices and users in the United States (Cao et al., 2020; Scanlan et al., 2019). The researcher developed four research questions to address this problem, with alternative and null hypotheses for each. These research questions focused on changes in cybersecurity risk for end-users of Starlink, whose primary customer base at the time of this study was rural populations (Musk, 2020). A risk-based theoretical methodology was used, with ISO 31000 as a guide.

A pre-and post-test design was used on human participants to conduct the research. Through survey instrumentation, specific questions relating to each research question were presented. The researcher allowed six months between the pre-and post-test surveys for adequate

treatment for each participant. Post-data collection results were analyzed and presented in Chapter 4 without concluding. It was found that changes did occur to the occurrence rates of identity theft, data breaches, reputational harm, malware, and virus infection for those who received the treatment and for the control group who did not. However, these results were determined to be not statistically significant.

The framework related to the results was analyzed. Additionally, recommendations were presented for SpaceX for Starlink end-user education and infrastructure threats. Specific areas for future research were also outlined to expand the body of knowledge within this field.

REFERENCES

Abbate, J. (2000). *Inventing the Internet*. MIT Press.

Abramson, N. (1985). Development of the ALOHANET. *IEEE Transactions on Information Theory*, *31*(2), 119–123. https://doi.org/10.1109/tit.1985.1057021

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1). https://doi.org/10.1093/cybsec/tyy006

Ahrens, F. (2003, April 10). *News corp. to buy Hughes, DirecTV*. The Washington Post. https://www.washingtonpost.com/archive/business/2003/04/10/news-corp-to-buy-hughes-directv/19a71119-fd61-4e14-8613-c17ed45d1624/

Alenezi, M., Alabdulrazzaq, H., Alshaher, A., & Alkharang, M. (2020). Evolution of malware threats and techniques: A review. *International Journal of Communication Networks and Information Security, 12*(3), 326–337.

Amazon. (2022). *Annual reports, proxies and shareholder letters.* Retrieved October 26, 2022, from https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx

American Psychological Association. (2020). *APA dictionary of psychology*. Retrieved October 26, 2022, from https://dictionary.apa.org/peer-review

Berlocher, G. (2009, September 1). *Minimizing latency in satellite networks*. Via Satellite. https://www.satellitetoday.com/telecom/2009/09/01/minimizing-latency-in-satellite-networks/

Blake, T. (2021, June 21). *Comparing cybersecurity frameworks*. Technology News and Information. https://seniordba.wordpress.com/2021/06/21/comparing-cybersecurity-frameworks/

Bonnor, N. (2012). A brief history of global navigation satellite systems. *The Journal of Navigation, 65*(1), 1–14. http://dx.doi.org/10.1017/S0373463311000506

Borthomieu, Y. (2014). Satellite lithium-ion batteries. In G. Pistoia (Eds.), *Lithium-ion batteries: Advances and applications* (pp. 311–14). Elsevier.

Brinkman, W., Haggan, D., & Troutman, W. (1997). A history of the invention of the transistor and where it will lead us. *IEEE Journal of Solid-State Circuits*, *32*(12), 1858–1865. https://doi.org/10.1109/4.643644

Brito, T., Celestino, C., & Moraes, R. (2013). A brief scenario about the "space pollution" around the Earth. *Journal of Physics: Conference Series, 465*. http://dx.doi.org/10.1088/1742-6596/465/1/012020

Brodkin, J. (2018, November 16). *FCC tells SpaceX it can deploy up to 11,943 broadband satellites*. Ars Technica. https://arstechnica.com/information-technology/2018/11/spacex-gets-fcc-approval-for-7500-more-broadband-satellites/

Brown, S. (1960). Project SCORE: Signal communication by orbiting relay equipment. *IRE Transactions on Military Electronics*, *MIL–4*(2/3), 193–194. https://doi.org/10.1109/iret-mil.1960.5008219

Brown, S., & Senn, G. (1960). Project SCORE. *Proceedings of the IRE*, *48*(4), 624–630. https://doi.org/10.1109/jrproc.1960.287438

Bugcrowd. (2022, March 1). *SpaceX's bug bounty program*. Retrieved October 26, 2022, from https://bugcrowd.com/spacex

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Campbell-Kelly, M., & Garcia-Swartz, D. (2013). The history of the Internet: The missing narratives. *Journal of Information Technology*, *28*(1), 18–33. https://doi.org/10.1057/jit.2013.4

Cao, H., Wu, L., Chen, Y., Su, Y., Lei, Z., & Zhao, C. (2020). *Analysis on the security of satellite Internet* [Paper presentation]. China Cyber Security Annual Conference 2020, Beijing, China.

Center for Strategic and International Studies. (2022). *Significant cyber incidents*. Retrieved October 26, 2022, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cerf, V. (2019). In debt to the NSF. *Communications of the ACM, 62*(4), 5–5. https://doi.org/10.1145/3313989

Cerf, V., Dalal, Y., & Sunshine, C. (1974). *RFC 675, Specification of Internet transmission control program.* https://datatracker.ietf.org/doc/html/rfc675

Chiba, Y. (2012). A simple method for sensitivity analysis of unmeasured confounding. *Journal of Biometrics & Biostatistics*, *3*(6). https://doi.org/10.4172/2155-6180.1000e113

Cohen-Almagor, R. (2011). Internet history. *International Journal of Technoethics*, *2*(2), 45–64. https://doi.org/10.4018/jte.2011040104

Committee on Government Reform. (2001). *What can be done to reduce the threats posed by computer viruses and worms to the working of the government?*

https://www.govinfo.gov/content/pkg/CHRG-107hhrg80480/html/CHRG-107hhrg80480.htm

Congressional-Executive Commission on China. (2011). *China's censorship of the Internet and social media: The human toll and trade impact*. https://www.govinfo.gov/content/pkg/CHRG-112hhrg72895/html/CHRG-112hhrg72895.htm

Conrath, C. (2004, February 19). Canadian firms take on Mydoom. *Network World Canada*. https://www.itworldcanada.com/article/canadian-firms-take-on-mydoom/14961

Cooper, M. (2019). GPS: The roots of its making and history. *ITNOW*, *61*(2), 20–21. https://doi.org/10.1093/itnow/bwz037

Creswell, J. (2012). *Educational research* (4th ed.). Pearson.

Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Creswell, J., & Guetterman, T. (2018). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.). Pearson.

Cybersecurity & Infrastructure Security Agency. (2020, June 30). *Securing network infrastructure devices.*. Retrieved October 26, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST18-001

Cybersecurity & Infrastructure Security Agency. (2021). *Federal information security modernization act.* Retrieved October 26, 2022, from https://www.cisa.gov/federal-information-security-modernization-act

Daehnick, C., Maritz, B., Wiseman, B., & Klinghoffer, I. (2020, May 04). Large LEO satellite constellations: Will it be different this time? *McKinsey & Company.* https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time

Dainow, E. (2017). *A concise history of computers, smartphones, and the Internet*. CreateSpace Independent Publishing Platform.

Dimitrov, D., & Rumrill, P., Jr. (2003). Pretest-posttest designs and measurement of change. *Work, 20*(2), 159–165.

Dinger, M., & Wade, J. T. (2019). The strategic problem of information security and data breaches. *The Coastal Business Journal, 17*(1), 1–25.

Dunbar, Brian. (2017). *What Is a Satellite?* NASA. https://www.nasa.gov/audience/forstudents/k-4/stories/nasa-knows/what-is-a-satellite-k4.html

Edmonds, W. & Kennedy, T. (2016). *An applied guide to research designs: Quantitative,*

Elburn, D. (2021, February 25). *LEO Economy FAQs*. NASA. https://www.nasa.gov/leo-economy/faqs/

Evans, B., Thompson, P., Corazza, G., Vanelli-Coralli, A., & Candreva, E. (2011). 1945–2010: 65 years of satellite history from early visions to latest missions. *Proceedings of the IEEE*, *99*(11), 1840–1857. https://doi.org/10.1109/jproc.2011.2159467

Falco, G. (2018). *The vacuum of space cyber security* [Paper presentation]. 2018 AIAA Space and Astronautics Forum and Exposition, Orlando, FL, United States.

Federal Bureau of Investigation. (2018, November 2). *The Morris worm*. Retrieved October 27, 2022, from https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Federal Bureau of Investigation. (2019). *2019 Internet crime report.* https://pdf.ic3.gov/2019_IC3Report.pdf

Federal Bureau of Investigation. (n.d.). *Common scams and crimes*. Retrieved October 27, 2022, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes

Federal Communications Commission (2015, February 4). *2015 broadband progress report.* https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2015-broadband-progress-report

Federal Communications Commission. (2010). *FCC 10-201: In the matter of preserving the open Internet broadband industry practices*. https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf

Federal Communications Commission. (2020). *OET exhibits list.* https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=tiQ8pAYT94LcLqmvDwsh8A%3D%3D&fcc_id=2AWHPR201

Federal Communications Commission. (2020, December 7). *Successful rural digital opportunity fund auction to expand broadband to over 10 million rural Americans* [Press release]. https://docs.fcc.gov/public/attachments/DOC-368588A1.pdf

Federal Communications Commission. (2021, February 8). *Starlink RDOF assessment.* https://ecfsapi.fcc.gov/file/10208168836021/FBA_LEO_RDOF_Assessment_Final_Report_20210208.pdf

Federal Communications Commission. (2021a). *Fourteenth broadband deployment report.* https://www.fcc.gov/reports-research/reports/broadband-progress-reports/fourteenth-broadband-deployment-report

Federal Communications Commission. (2021b). *Petition of Starlink services, LLC for designation as an eligible telecommunications carrier.* https://ecfsapi.fcc.gov/file/1020316268311/Starlink%20Services%20LLC%20Application%20for%20ETC%20Designation.pdf

Federal Communications Commission. (2021c). *Order and authorization and order on reconsideration*. https://docs.fcc.gov/public/attachments/FCC-21-48A1.pdf

Federal Communications Commission. (2022). *Application for fixed satellite service by SpaceX Services, Inc.* https://fcc.report/IBFS/SES-LIC-20200714-00758

Foust, J., & Berger, B. (2022, March 5). *SpaceX shifts resources to cybersecurity to address Starlink jamming*. SpaceNews. https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/

Frey, B. (2018). *The SAGE encyclopedia of educational research, measurement, and evaluation (Vols. 1–4).* SAGE Publications, Inc. https://doi.org/10.4135/9781506326139

Garber, L. (1999). Melissa virus creates a new type of threat. *Computer*, *32*(6), 16–19. https://doi.org/10.1109/mc.1999.769438

Garner, R. (2022). *About - Hubble history timeline*. NASA. https://www.nasa.gov/content/goddard/hubble-timeline-full-text

Garrity, J., & Husar, A. (2021). *Digital connectivity and low earth orbit satellite constellations: Opportunities for Asia and the Pacific*. Asian Development Bank.

Gartner. (n.d.). *Gartner Information Technology Glossary*. https://www.gartner.com/en/information-technology/glossary

Geers, K. (2011). *Strategic cyber security*. NATO Cooperative Cyber Defence Centre of Excellence Publications.

Gerencer, T. (2020, November 4). *The top 10 worst computer viruses in history*. HP. https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history

Gilroy, A., & Kruger, L. (2006). *Broadband Internet regulation and access: Background and issues.* Congressional Research Service. https://www.everycrsreport.com/files/20060126_IB10045_34fdbf70cdd3e1861f15cd4a3e5c7f6d26539c7b.pdf

Grabosky, P. (2006). Editor's introduction*. Crime, Law and Social Change, 46*, 185–187. https://doi.org/10.1007/s10611-007-9062-8

Gupta, C., & Kumar, D. (2020). Identity theft: A small step towards big financial crimes. *Journal of Financial Crime, 27*(3), 897–910. http://dx.doi.org/10.1108/JFC-01-2020-0014

Hamilton, L. (2017). Let me tell you who I am: Establishing a federal remedy for interference with online identity. *Federal Communications Law Journal, 69*(2), 173.

Hofer-Schmitz, K., Kleb, U., & Stojanovic, B. (2021). The influences of feature sets on the detection of advanced persistent threats. *Electronics, 10*(6), 704. https://doi.org/10.3390/electronics10060704

Homeland Security. (2021, August 08). *What is personally identifiable information?* [Video]. https://www.dhs.gov/privacy-training/what-personally-identifiable-information https://www.proquest.com/openview/1b8585c293a3531bddee852acb9e7877/1.pdf?pq-origsite=gscholar&cbl=40767

Hughes Corporate (n.d.). *About Hughes*. Retrieved October 27, 2022, from https://www.hughes.com/about

Hughes-Lartey, K., Li, M., Botchey, F., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Hung, W. (2021, May 13). *SpaceX is in search for more Taiwanese suppliers*. TechTaiwan. https://techtaiwan.com/20210513/spacex-taiwanese-suppliers/

Identity Theft Resource Center. (2022). *Breach trends*. Retrieved October 27, 2022, from https://notified.idtheftcenter.org/s/

Information Commissioner's Office. (n.d.). *Personal data breaches*. Retrieved October 27, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa

International Astronomical Union. (2020). *Satellite constellations.* Retrieved October 27, 2022, from https://www.iau.org/public/themes/satellite-constellations/#introduction

International Organization for Standardization. (2015). *ISO/IEC 27040:2015*. Retrieved October 27, 2022, from https://www.iso.org/standard/44404.html

International Organization for Standardization. (2018). *ISO 31000:* 2018. Retrieved October 27, 2022, from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Iridium. (2022). *History of Iridium.* https://www.iridiummuseum.com/timeline/

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods, 8*(4), 49–62. https://doi.org/10.1177/160940690900800406

Janjarasjit, S., & Chan, S. (2021). Reaction of users as potential victims of information security breach. *Information and Computer Security, 29*(1), 187–206. http://dx.doi.org/10.1108/ICS-07-2020-0118

Jensen, E., Jones, N., Rabe, M., Pratt, B., Medina, L., Orozco, K., & Spell, L. (2021, August 12). The chance that two people chosen at random are of different race or ethnicity groups has increased since 2010. *United States Census Bureau.* Retrieved October 27, 2022, from https://www.census.gov/library/stories/2021/08/2020-united-states-population-more-racially-ethnically-diverse-than-2010.html

Kaspersky. (2021, May 26). *Turla hiding in the sky: Russian speaking cyberespionage group exploits satellites to reach the ultimate level of anonymity* Retrieved October 27, 2022, from https://www.kaspersky.com/about/press-releases/2015_turla-hiding-in-the-sky-russian-speaking-cyberespionage-group-exploits-satellites-to-reach-the-ultimate-level-of-anonymity

Kim, J., & Choi, I. (2021). Choosing the level of significance: A decision-theoretic approach. *Abacus*, *57*(1), 27–71. https://doi.org/10.1111/abac.12172

Koumartzis, N., & Veglis, A. (2011, June 28–July 1*). On the pursue for a fair Internet regulation system: A blueprint for a content blocking system encouraging participation by the Internet user*s [Paper presentation]. 2011 IEEE Symposium on Computers and Communications, Kerkyra, Greece.

Le Doan, D., Amyotte, E., Mok, C., & Uher, J. (2004, July). *Anik-F2 Ka-band transmit multibeam antenna* [Paper presentation]. 2004 10th International Symposium on Antenna Technology and Applied Electromagnetics and URSI Conference, Ottawa, ON, Canada.

Library of Congress Archives. (2004). *International agreements and domestic legislation affecting freedom of expression.* http://webarchive.loc.gov/all/20040623205930/http://www.cecc.gov/pages/virtualAcad/exp/explaws.php

Los Angeles Business Journal (2005, November 9). *DirecTV sells Hughes stake to SkyTerra.* Retrieved October 27, 2022, from https://labusinessjournal.com/news/2005/nov/10/directv-sells-hughes-stake-to-skyterra/

Ludvigsen, M., Hall, E., Meyer, G., Fegran, L., Aagaard, H., & Uhrenfeldt, L. (2016). Using Sandelowski and Barroso's meta-synthesis method in advancing qualitative evidence. *Qualitative Health Research 26*(3), 320–29. https://doi.org/10.1177%2F1049732315576493

Luminita, H., Mihai, N. Cristina, M., & Marin, T. (2022). Cost-benefit analysis (cba)-key factor in evaluation of investment products. *Journal of Information Systems & Operations Management, 16(1),* 88–101.

Lundgren, B., & Möller, N. (2019). Defining information security. *Science and Engineering Ethics, 25*, 419–441. http://dx.doi.org/10.1007/s11948-017-9992-1

Maitlo, A., Ameen, N., Peikari, H. R., & Shah, M. (2019). Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. *Information Technology & People, 32*(5), 1184–1214. http://dx.doi.org/10.1108/ITP-05-2018-0255

Manulis, M., Bridges, C., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in new space. *International Journal of Information Security, 20*, 287–311. https://doi.org/10.1007/s10207-020-00503-w

McGlade, D. (2010). Commercial operators partnering with the military to meet global bandwidth demands. *High Frontier*, *6*(2), 1–58. https://www.afspc.af.mil/Portals/3/documents/HF/AFD-100226-085.pdf

Meinel, C., & Sack, H. (2014). *Digital communication: Communication, multimedia, security* (2014th ed.). Springer.

Meta. (2022). *About Facebook*. Retrieved October 27, 2022, from https://about.facebook.com/technologies/facebook-app/

Metcalfe, R., & Boggs, D. (1976). Ethernet: Distributed packet switching for local computer networks. *Communications of the ACM*, *19*(7), 395–404. https://doi.org/10.1145/360248.360253

Middleton, B. (2017). *A history of cyber security attacks: 1980 To present*. Auerbach Publications.

Miller, A. (2021, Nov 30). *Satellite internet latency: What's the big deal?* Viasat. Retrieved October 27, 2022, from https://www.viasat.com/about/newsroom/blog/satellite-internet-latency-whats-the-big-deal/

Mockapetris, P. (1983). *RFC 882, Domain names – concepts and facilities*.

Musk, E. (2020, March 9-12). *Keynote presentation*. Satellite 2020, Washington DC, United States.

Musk, E. [@Elonmusk]. (2019, May 11). *First 60 @SpaceX starlink satellites loaded into Falcon fairing. Tight fit*. [Tweet]. Twitter. https://twitter.com/elonmusk/status/1127388838362378241

NASA. (2002). *Switchboard in the sky*. Retrieved October 27, 2022, from https://www.nasa.gov/centers/glenn/about/fs13grc.html

NASA. (2008, March 28). *The birth of NASA*. https://www.nasa.gov/exploration/whyweexplore/Why_We_29.html

National Institute of Standards and Technology. (2018). *Getting started*. Retrieved October 27, 2022, from https://www.nist.gov/cyberframework/getting-started

National Institute of Standards and Technology. (n.d.). *Glossary | CSRC*. https://csrc.nist.gov/glossary

National Research Council. (2013). *Landsat and beyond: Sustaining and enhancing the nation's land imaging program*. National Academies Press. https://doi.org/10.17226/18420

National Science Foundation. (2003, August 13). *A Brief History of NSF and the Internet*.. https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Pearson Education.

Newell, H. (2009). *Beyond the atmosphere: Early years of space science*. Dover Publications.

OneWeb. (2021, December 27). *OneWeb confirms successful launch of 36 satellites, after rapid year of progress*. [Press release]. https://oneweb.net/media-center/oneweb-confirms-successful-launch-of-36-satellites-after-rapid-year-of-progress

Osanloo, A., & Grant, C. (2016). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." *Administrative Issues Journal: Connecting Education, Practice, and Research, 4*(2). https://doi.org/10.5929/2014.4.2.9

Pachler, N., del Portillo, I., Crawley, E., & Cameron, B. (2021). *An updated comparison of four low earth orbit satellite constellation systems to provide global broadband* [Paper

presentation]. 2021 IEEE International Conference on Communications Workshops, Montreal, QC, Canada.

Pannucci, C. & Wilkins, E. (2010). Identifying and avoiding bias in research. *Plastic and reconstructive surgery*, *126*(2), 619–625. https://doi.org/10.1097/PRS.0b013e3181de24bc

Pavur, J. (2020, August 5). *Whispers among the stars: Perpetrating (and preventing) satellite eavesdropping attacks* [Conference session]. Black Hat USA, Las Vegas, NV, United States. https://i.blackhat.com/USA-20/Wednesday/us-20-Pavur-Whispers-Among-The-Stars-Perpetrating-And-Preventing-Satellite-Eavesdropping-Attacks.pdf

Pelton, J. (2010). The start of commercial satellite communications. [History of communications]. *IEEE Communications Magazine*, *48*(3), 24–31. https://doi.org/10.1109/mcom.2010.5434368

Perrin, A., & Duggan, M. (2015). *Americans' Internet access: 2000-2015*. Pew Research Center. https://www.pewresearch.org/internet/2015/06/26/americans-internet-access-2000-2015/

Pope, M., Warkentin, M., Mutchler, L., & Luo, X. (2012). The domain name system—past, present, and future. *Communications of the Association for Information Systems*, *30*. https://doi.org/10.17705/1cais.03021

Posadzki, A. (2020, September 22). *Internet everywhere, but at a cost: The race for the low-earth satellite market*. The Globe and Mail. Technology. Retrieved October 27, 2022, from https://www.theglobeandmail.com/business/article-internet-everywhere-but-at-a-cost-the-race-for-the-low-earth/

qualitative, and mixed methods. Sage Publications, Inc.

Riebeek, H. (2009, September 4). *Catalog of earth satellite orbits*. NASA Earth Observatory. https://earthobservatory.nasa.gov/features/OrbitsCatalog#:~:text=Inclination%20is%20the%20angle%20of,its%20inclination%20is%2090%20degrees

Rogers, D., Ippolito, L., & Davarian, F. (1997). System requirements for Ka-band earth-satellite propagation data. *Proceedings of the IEEE*, *85*(6), 810–820. https://doi.org/10.1109/5.598406

Rotzal, P. (2002). *X.400 message handling system: The remote user agent* [Paper presentation]. Milcom '95, San Diego, CA, United States. https://doi.org/10.1109/MILCOM.1995.483504

Rueter, J. (2019, August 13). *A brief history of Internet service providers*. Viasat. Retrieved October 27, 2022, from https://www.viasat.com/about/newsroom/blog/a-brief-history-of-internet-service-providers/

Ryan, J. (2010). *From military networks to the global Internet*. Reaktion Books.

Ryan, J. (2013). *A history of the Internet and the digital future*. Reaktion Books.

Saif, U., Chudhary, A. Butt, S., & Butt, N. (2007). Poor man's broadband: Peer-to-peer dialup networking. *Computer Communication Review*, *37*(5), 5–16. https://doi.org/10.1145/1290168.1290170

Saint-Germain, M. (n.d.). *Experimental designs for research*. https://homeweb.csulb.edu/%7Emsaintg/ppa696/696exper.htm

Salkind, N. (2010). *Encyclopedia of research design*. SAGE Publications, Inc. https://doi.org/10.4135/9781412961288

Salkind, N. J. (2017). *Exploring research* (9th ed.). Pearson.

SatelliteMap.Space. (2022, February 22). *Starlink satellite tracker* https://satellitemap.space/?constellation=starlink

Scanlan, J., Styles, J., Lyneham, D., & Lützhöft, M. (2019). *New Internet satellite constellations to increase cyber risk in ill-prepared industries* [Paper presentation]. 70th International Astronautical Congress. Washington DC, United States.

Seemma, P., Nandini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11). https://doi.org/10.17148/ijarcee.2018.71127

Seymour, T., & Shaheen, A. (2011). History of wireless communication. *Review of Business Information Systems, 15*(2), 37–42.

Sheetz, M. (2021a, January 29). *SpaceX looks to build next-generation Starlink internet satellites after launching 1,000 so far*. CNBC. Retrieved October 27, 2022, from https://www.cnbc.com/2021/01/28/spacex-plans-next-generation-starlink-satellites-with-1000-launched.html

Sheetz, M. (2021b, August 3). *SpaceX says Starlink has about 90,000 users as the internet service gains subscribers*. CNBC. Retrieved October 27, 2022, from https://www.cnbc.com/2021/08/03/spacex-starlink-satellite-internet-has-about-90000-users.html

Sheetz, M. (2021c, February 9). *Telesat to build a $5 billion global satellite network to bring fiber-like internet to businesses*. CNBC. Retrieved October 27, 2022, from https://www.cnbc.com/2021/02/09/telesat-building-5-billion-lightspeed-global-satellite-internet.html

Sheetz, M. (2021d, November 5). *In race to provide internet from space, companies ask FCC for about 38,000 new broadband satellites*. CNBC. Retrieved October 27, 2022, from https://www.cnbc.com/2021/11/05/space-companies-ask-fcc-to-approve-38000-broadband-satellites.html

Sheetz, M. (2022, January 6). *SpaceX's Starlink Internet service has more than 145,000 users so far*. CNBC. Retrieved October 27, 2022, from https://www.cnbc.com/2022/01/06/spacex-starlink-internet-service-has-more-than-145000-users-so-far.html

Shirey, R. (2007). *Internet security glossary* (Version 2). Internet Engineering Task Force. https://doi.org/10.17487/RFC4949

Siddiqi, A. (2011). *Challenge to Apollo: The Soviet Union and the space race, 1945–1974*. Military Bookshop.

Simon, M., & Goes, J. (2010). *Dissertation and scholarly research: Recipes for success*. CreateSpace Independent Publishing.

Slotten, H. R. (2015). International governance, organizational standards, and the first global satellite communication system. *Journal of Policy History, 27*(3), 521–549. http://dx.doi.org/10.1017/S0898030615000214

Smith, G. (2015). Management models for international cybercrime. *Journal of Financial Crime*, *22*(1), 104–125. https://doi.org/10.1108/jfc-09-2013-0051

Solove, D., & Citron, D. (2018). Risk and anxiety: A theory of data-breach harms. *Texas Law Review, 96*(4), 737–786.

Space Exploration Technologies Corporation. (2021). *SpaceX non-geostationary satellite system*. https://fcc.report/IBFS/SAT-MOD-20181108-00083/1569860.pdf

SpaceX. (2022). *Launches.* https://www.spacex.com/launches/

Spinello, R. (2021). Corporate data breaches: A moral and legal analysis. *Journal of Information Ethics, 30*(1), 12–32. http://dx.doi.org/10.2307/JIE.30.1.12

Spurgeon, C. (2000). *Ethernet: The definitive guide* (1st ed.). O'Reilly Media.

Starlink. (2022). *Specifications & Configurations*. Retrieved October 27, 2022, from https://support.starlink.com/topic?category=10

Stein, J. (2021). *2020 data breach report*. North Carolina Department of Justice. https://ncdoj.gov/wp-content/uploads/2021/01/2020-NCDOJ-Data-Breach-Report.pdf

Sturdevant, R. (2014). You are here: From the compass to GPS, the history and future of how we find ourselves. *Air Power History, 61*(3), 50.

SurveyMonkey (2022). *Are my survey responses anonymous and secure?* SurveyMonkey. Retrieved October 27, 2022, from https://help.surveymonkey.com/articles/en_US/kb/Are-my-survey-responses-anonymous-and-secure

Swenson, G. (1997). Looking back: Sputnik. *IEEE Potentials, 16*(1), 36–40. https://doi.org/10.1109/45.565615

Takei, J., & Murai, J. (2003, January 27–31). *Satellite communication on the Internet: Its history and the technology* [Conference Session]. 2003 Symposium on Applications and the Internet Workshops, Orlando, FL, United States. https://doi.org/10.1109/saintw.2003.1210116

Telesat (2020, May 20). *Telesat lightspeed*. Retrieved October 27, 2022, from https://www.telesat.com/leo-satellites/

Teodorescu, C. (2022). Perspectives and reviews in the development and evolution of the zero-day attacks. *Informatica Economica, 26*(2), 46–56. https://doi.org/10.24818/issn14531305/26.2.2022.05

Terzi, N. (2011). The impact of e-commerce on international trade and employment. *Procedia-Social and Behavioral Sciences, 24*, 745–753. https://doi.org/10.1016/j.sbspro.2011.09.010

The Business Research Company. (2021). *Low earth orbit (leo) satellites global market report.* (2021). https://www.thebusinessresearchcompany.com/report/low-earth-orbit-leo-satellites--global-market-report

The European Space Agency. (2020). *Low earth orbit*. https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit

The European Space Agency. (2020, March 30). *Types of orbits.* https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

The European Space Agency. (n.d.). *Satellite frequency bands.* https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands

The United States Department of Justice. (2020). *Identity theft*. Retrieved October 27, 2022, from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing, 7*(3), 155–162. http://doi.org/10.5281/zenodo.2552022

Tikito, I., & Souissi, N. (2019). Meta-analysis of systematic literature review methods. *International Journal of Modern Education and Computer Science, 11*(2), 17–25. http://dx.doi.org/10.5815/ijmecs.2019.02.03

United Nations Office for Outer Space Affairs (2022). *Committee on the Peaceful Uses of Outer Space.* https://www.unoosa.org/oosa/en/ourwork/copuos/index.html

United States Census Bureau (2021). *2010 census urban and rural classification and urban area criteria*. (2021). https://www.census.gov/programs-surveys/geography/guidance/geo-areas/urban-rural/2010-urban-rural.html

United States Census Bureau. (2022). *Quick facts: United States*. https://www.census.gov/quickfacts/fact/table/US/HCN010212

United States Government Accountability Office. (2004, September). *Telecommunications: Intelsat privatization and the implementation of the ORBIT Act* (GAO-04-891).

United States Government Publishing Office (2022). *Communications satellite act of 1962*, Pub. L. No 87-624, Stat. 76 (1964). https://www.govinfo.gov/content/pkg/STATUTE-76/pdf/STATUTE-76-Pg419.pdf

University of Southern California. (1981a). *RFC 791, Internet control protocol.* https://datatracker.ietf.org/doc/html/rfc791

University of Southern California. (1981b). *RFC 793, transmission control protocol.* https://datatracker.ietf.org/doc/html/rfc793

USGS. *What is the Landsat satellite program and why is it important?* https://www.usgs.gov/faqs/what-landsat-satellite-program-and-why-it-important

Vanderweele, T. J., & Arah, O. A. (2011). Bias formulas for sensitivity analysis of unmeasured confounding for general outcomes, treatments, and confounders. *Epidemiology,* 22(1), 42–52. https://doi.org/10.1097/EDE.0b013e3181f74493

Voelsen, D. (2021). *Internet from space: How new satellite connections could affect global Internet governance*. German Institute for International and Security Affairs. https://doi.org/10.18449/2021RP03

Wall, M. (2021, November 2). Amazon to launch 1st prototype Internet satellites for Kuiper constellation in 2022. *Space*. https://www.space.com/amazon-kuiper-prototype-internet-satellites-launch-2022

Webb, J. (2015). James Webb, son of Hubble. *Engineering & Technology*, *10*(4), 66–69. https://doi.org/10.1049/et.2015.0422

Weiner, I. (2003). *Handbook of psychology*. John Wiley & Sons.

Weiss, A. (2004). Trends for 2005. *NetWorker*, *8*(4), 20–27. https://doi.org/10.1145/1037911.1037912

Wigand, R. (1997). Electronic commerce: Definition, theory, and context. *The Information Society, 13*(1), 1–16. https://doi.org/10.1080/019722497129241

Wright, J. (2001). *International encyclopedia of the social & behavioral sciences*. Pergamon Press.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. http://dx.doi.org/10.1177/0739456X17723971

Yen, L. (2002). Satellite communications for the millennium. *IEEE Antennas and Propagation Society International Symposium. Transmitting Waves of Progress to the Next Millennium. 2000 Digest. Held in Conjunction with: USNC/URSI National Radio Science Meeting (Cat. No.00CH37118)*.

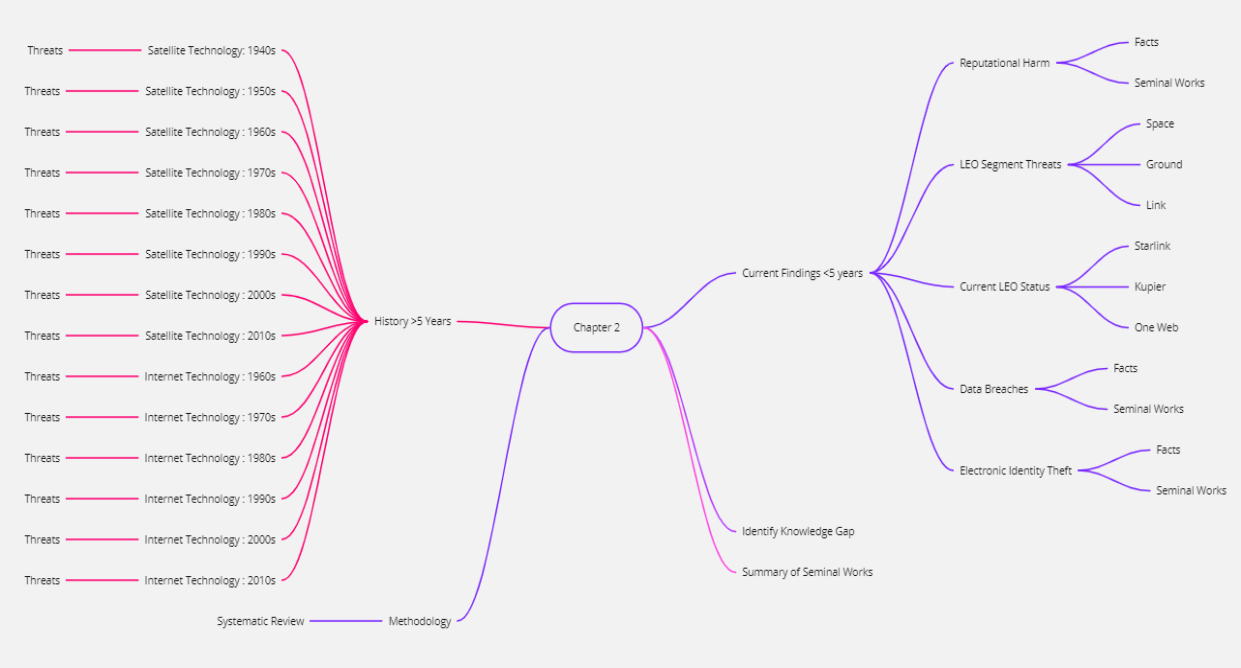
Yu, W., & Qian, X. (2010, October 22–24). *Communication satellite orbit and Iridium satellite plan's restarting* [Paper presentation]. 2010 International Conference on Computer Application and System Modeling, Taiyuan, China.

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*. https://doi.org/10.48550/ARXIV.2201.03063

Zhong, F., Chen, Z., Xu, M., Zhang, G., Yu, D., & Cheng, X. (2022). Malware-on-the-brain: Illuminating malware byte codes with images for malware classification. *IEEE Transactions on Computers, 1*(1). https://doi.org/10.1109/tc.2022.3160357

Zou, Y., Roundy, K., Tamersoy A., Shintre, S., Roturier, J., & Schaub, F. (2020, April 25–30). *Examining the adoption and abandonment of security, privacy, and identity theft protection practices* [Paper presentation]. 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, United States. https://doi-org./10.1145/3313831.3376570

APPENDIX A: LITERATURE REVIEW MAP



APPENDIX B: PRE-TEST SURVEY

Starlink Cybersecurity Risk Survey (Pre-Test)

The purpose of this research project is to determine possible cybersecurity risks associated with the use of Starlink. Your participation in this survey is 100% voluntary. You may choose not to participate and can withdraw at any time.

By continuing with this survey, you certify that you are aged at least 18 years, have the legal capacity to give consent, and are able to exercise free power of choice.

This data collection is for research purposes only and is not affiliated with Starlink or SpaceX companies.

An approved IRB is on file at Capitol Technology University.

For any questions regarding this survey, please email Chris Gerber (cjgerber@captechu.edu).

* 1. Are you at least 18 years old?

- ◯ Yes
- ◯ No

Starlink Cybersecurity Risk Survey (Pre-Test)

* 2. Have you pre-ordered, but not yet installed Starlink?

- ◯ Yes
- ◯ No

Starlink Cybersecurity Risk Survey (Pre-Test)

* 3. What is your Zip Code?

* 4. What is your email address?

* 5. How many people are in your household?

- 1
- 2
- 3
- 4
- Specify Number

* 6. Do you currently have access to High-Speed Internet (minimum 25Mbps download/3Mbps upload) at your residence?

- Yes
- No
- Not Sure

Starlink Cybersecurity Risk Survey (Pre-Test)

* 7. How long have you had High Speed Internet access at your residence?

- 1 Year or Less
- 2 years or Less
- Greater Than 2 years

* 8. Once Starlink is installed at your residence do you expect your Internet usage to increase?

- Yes
- No
- No Change

* 9. In the past 24 months, have you been a victim of identity theft?

Examples include:

- Financial Accounts opening in your name without permission
- Denied Credit based on false information
- Unauthorized bank transactions
- Unauthorized communication for accounts you don't recognize

- ◯ Yes
- ◯ No

Starlink Cybersecurity Risk Survey (Pre-Test)

* 10. How many incidents of identity theft have you experienced?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 11. In the past 24 months, have you discovered that someone had misused or attempted to misuse your personal information?

Examples include:

- Access to your personal data without permission
- Modification of personal data without permission
- Personal data lost or stolen

- ◯ Yes
- ◯ No

* 12. How many incidents of misuse or attempted misuse of your personal information have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 13. In the past 24 months, have you experienced any harm to your reputation?

Examples include:

- False perceptions of your character causing harm to social media presence
- False perceptions of your character causing harm to personal financial accounts and/or credit

- ◯ Yes
- ◯ No

Starlink Cybersecurity Risk Survey (Pre-Test)

* 14. How many incidents of harm to your reputation have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 15. In the past 24 months, how many incidents of a virus or malware have you seen on endpoints (computers, laptops, tablets, phones) in your household?

- 0
- 1
- 2
- 3
- Specify Number

Thank you for completing this survey! In approximately 6 months, a follow-up email will be sent out to the address you provided with a link to a follow-up survey. A response is required in order to qualify for the gift card drawing.

APPENDIX C: POST-TEST SURVEY

Starlink Cybersecurity Risk Survey (Post-Test)

1.

The purpose of this research project is to determine possible cybersecurity risks associated with the use of Starlink. Your participation in this survey is 100% voluntary. You may choose not to participate and can withdraw at any time.

By continuing with this survey, you certify that you are aged at least 18 years, have the legal capacity to give consent, and are able to exercise free power of choice.

This data collection is for research purposes only and is not affiliated with Starlink or SpaceX companies.

An approved IRB is on file at Capitol Technology University.

All information collected will be kept confidential and transmitted using secure methods. If you have any questions regarding this survey, please contact Chris Gerber (cjgerber@captechu.edu).

* 1. Are you at least 18 years old?

- ◯ Yes
- ◯ No

* 2. What is your Zip Code?

* 3. What is your email address?

* 4. How many people are in your household?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 5. Have you purchased and installed Starlink at your residence?

- ◯ Yes
- ◯ No

* 6. Approximately when did you install and first use it?

* 7. Since installation of Starlink, have you been a victim of identity theft?

Examples include:

- Financial Accounts opening in your name without permission
- Denied Credit based on false information
- Unauthorized bank transactions
- Unauthorized communication for accounts you don't recognize

- ◯ Yes
- ◯ No

* 8. Since your installation of Starlink, how many incidents of identity theft have you experienced?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 9. Since installation of Starlink, have you discovered that someone had misused or attempted to misuse your personal information?

Examples include:

- Access to your personal data without permission
- Modification of personal data without permission
- Personal data lost or stolen

- ◯ Yes
- ◯ No

* 10. Since installation of Starlink, how many incidents of misuse or attempted misuse of your personal information have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 11. Since installation of Starlink, have you experienced any harm to your reputation?

Examples include:

- False perceptions of your character causing harm to social media presence
- False perceptions of your character causing harm to personal financial accounts and/or credit

- ◯ Yes
- ◯ No

* 12. Since installation of Starlink, how many incidents of harm to your reputation have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 13. Since installation of Starlink, how many incidents of a virus or malware have you seen on endpoints (computers, laptops, tablets, phones) in your household?

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ Specify Number

Starlink Cybersecurity Risk Survey (Post-Test)

2. Non-Starlink Install (Control Group)

* 14. Do you currently have access to High-Speed (minimum 25Mbps download/3Mbps upload) Internet at your residence?

- ◯ Yes
- ◯ No
- ◯ Not Sure

* 15. How long have you had High Speed Internet access at your residence?

- ◯ 1 Year or Less
- ◯ 2 years or Less
- ◯ Greater Than 2 years

* 16. In the past 6 months, have you been a victim of identity theft?

Examples include:

- Financial Accounts opening in your name without permission
- Denied Credit based on false information
- Unauthorized bank transactions
- Unauthorized communication for accounts you don't recognize

- ◯ Yes
- ◯ No

* 17. In the past 6 months, how many incidents of identity theft have you experienced?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

[ ]

* 18. In the past 6 months, have you discovered that someone had misused or attempted to misuse your personal information?

Examples include:

- Access to your personal data without permission
- Modification of personal data without permission
- Personal data lost or stolen

- ◯ Yes
- ◯ No

* 19. In the past 6 months, how many incidents of misuse or attempted misuse of your personal information have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 20. In the past 6 months, have you experienced any harm to your reputation?

Examples include:

- False perceptions of your character causing harm to social media presence
- False perceptions of your character causing harm to personal financial accounts and/or credit

- ◯ Yes
- ◯ No

* 21. In the past 6 months, how many incidents of harm to your reputation have occurred?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ Specify Number

* 22. In the past 6 months, how many incidents of a virus or malware have you seen on endpoints (computers, laptops, tablets, phones) in your household?

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ Specify Number

APPENDIX D: PILOT STUDY ADDITIONAL QUESTIONS

16. How satisfied are you with the look and feel of this survey??

- ◯ Extremely satisfied
- ◯ Very satisfied
- ◯ Somewhat satisfied
- ◯ Not so satisfied
- ◯ Not at all satisfied

17. What did you like about the survey?

18. What did you dislike about the survey?

19. Any additional comments to share with the researcher to help improve this survey?