5-3-2024

Strategies to Rapidly Decommission Information Technology Satellites to Prevent Low Earth Orbit Space Debris

Nathaniel Richard Juarez
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Nathaniel Richard Juarez

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Constance Blanson, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Strategies to Rapidly Decommission Information Technology Satellites to Prevent Low Earth Orbit Space Debris

by

Nathaniel Richard Juarez

MS, American Military University 2017

BS, American Military University 2015

AA, American Military University 2017

AS, American Military University 2018

AAS, Community College of the Air Force 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2024

Abstract

Information technology (IT) assets rely heavily on satellites in space, with most of them in low Earth orbit (LEO). There is a growing threat towards IT satellites in LEO and cybersecurity professionals must implement proactive measures through policy reform and hardening procedures to prevent cyberattacks. The Kessler syndrome will become existent if satellites start crashing into each other or space debris orbiting the Earth. Grounded in the integrated system theory of information security management, the purpose of this qualitative pragmatic inquiry was to explore strategies IT satellite managers in the space industry use to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. The participants comprised eight cyber security professionals across the southeastern states of the United States. Data were collected using interviews and analyzed using a modified van Kaam method. Three themes were identified: (a) policy concerns, (b) system hardening/logistics and current decommissioning for IT satellites and supporting systems, and (c) legacy equipment. A key recommendation for cyber security professionals is to remove outdated/legacy equipment from space. The implications for positive social change include the potential for more efficient and sustainable use of space resources, a reduction of space debris, and protection of space assets from cyber-attacks.

Strategies to Rapidly Decommission Information Technology Satellites to Prevent Low Earth Orbit Space Debris

by

Nathaniel Richard Juarez

MS, American Military University 2017

BS, American Military University 2015

AA, American Military University 2017

AS, American Military University 2018

AAS, Community College of the Air Force 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2024

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Information technology (IT) capabilities rely heavily on space satellites orbiting the Earth, and these satellites are vulnerable to disasters due to manufactured attacks in the cyberworld, fuel loss, or miscalculations of positioning (Mitrea et al., 2020). Due to these vulnerabilities, satellites require hardening and countermeasures from becoming susceptible to cyberattacks or collisions to become space debris. Furthermore, the problem of space debris is a global issue, with every country facing potential dangers in space if collisions occur. One nation's actions could have dire consequences for other nations if a large amount of space debris is created. Researchers, satellite manufacturers, rocket producers, and IT professionals have been looking into ways to rapidly decommission satellites out of orbit without generating more or any space debris, and the methods to do so could include but are not limited to lasers, nets, chemical spray, and magnetics (Raguraman et al., 2020).

Problem Statement

Low Earth orbits (LEOs) are vulnerable to disasters due to manufactured attacks in the cyberworld, fuel loss, or miscalculations of positioning (Mitrea et al., 2020). LEO satellites deployed by the space industry are in danger of a potentially irreversible rippling effect of satellites continuously crashing into each other if probable collisions occur which is known as the Kessler Syndrome (R. Wang et al., 2020). According to the National Aeronautics and Space Administration (NASA), there will be a 75% increase in space debris in LEO traveling up to 17,500 mph, and the space industries are expecting to

experience more frequent satellite collisions by 2030 (Torky et al., 2019). The general IT problem that prompted me to conduct this study is LEO satellite collisions and cyberattacks could affect all humans who rely on satellites for their operations. The specific IT problem was that some IT satellite managers in the space industry lack strategies to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks.

Purpose Statement

The purpose of this qualitative pragmatic inquiry study was to explore strategies used by IT satellite managers in the space industry to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. The participants are current and prior contractors working for space agencies with experience in satellite operations and manufacturing. The geographical location of the study was the surrounding areas of Cape Canaveral, Florida. Implications for positive social change include the shift in focus for space agencies across the globe to (a) potentially clean space debris before crashing debris hurts those on Earth, (b) link several nations together with the goal of not generating space debris, and (c) use new technologies to prevent satellites from becoming weaponized.

Nature of the Study

I selected a qualitative methodology for this study. Use of the qualitative method allows for a deep understanding of a problem and attempts to clarify how people think (Ratnapalan, 2019). I used the qualitative method to explore strategies used by IT satellite managers to properly and rapidly decommission satellites out of LEO. The quantitative

research method is used to test and prove hypotheses and conduct experiments (Seeber, 2020). I did not test any hypotheses or conduct any experiments. Since qualitative research yielded enough in-depth understanding of the research question, there was no need for statistical measurements (see Nair & Prem, 2020). I did not seek to conduct any statistical measurements; therefore, a mixed-methods approach was not appropriate for the study.

To address the research questions in this qualitative study, I employed a pragmatic inquiry design. This approach was appropriate for this study because it could be applied to experience-based scenarios, and I tailored it to explore how individuals or organizational experiences have been shaped through social interaction. The pragmatic inquiry design may include interviews and observations made by individuals with experience (Kelly & Cordeiro, 2020). A pragmatic study concentrates on an individual decision maker within real-world situations to identify gaps, opportunities, and challenges to guide future research (Ferrer & Ellis, 2019). A case study is an in-depth and detailed study of one person, group, or event (Crowe et al., 2011). I did not select a case study design for this study because more than a single person, group, or event were being analyzed. A phenomenological study is conducted to explore what individuals have experienced and is focused on their experience of a phenomena (Neubauer et al., 2019). A phenomenological design was not selected for this study because the Kessler syndrome phenomena has not occurred, meaning no one could be interviewed about experiencing it.

Research Question

What strategies do IT satellite managers in the space industry use to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks?

Interview Questions

I used the following semi-structured interview questions to explore the phenomenon, with the intention of gathering answers that directly related to the research question.

1. What is the importance of preventing space debris?
2. What methods are used to prevent space debris?
3. What strategies are used to properly harden satellites against cyberattacks?
4. What strategies are used to rapidly decommission satellites out of LEO?
5. What would happen if the Kessler syndrome started, and can we prevent it?
6. What is the dependency of space operations on Earth's population?
7. In your opinion, what different strategies would provide a better end result versus what is being used?
8. What strategies do IT satellite managers use to decommission satellites out of LEO if targeted by cyberattacks?
9. What administrative policies are in place to stop cyberattacks? Are they working?
10. Would you like to provide any additional information on cyber strategies or comments regarding rapidly decommissioning satellites out of LEO?

Conceptual Framework

I used Hong et al.'s (2003) integrated system theory of information security management (ISTISM) as the conceptual framework of this study to identify information security strategies and procedures to improve information security. The ISTISM framework has wide-ranging applicability in the investigation of cybersecurity management issues because it incorporates and considers multiple frameworks utilized in various studies. The components of the ISTISM framework related to the research problem in the current study because it integrates security policies, risk management, and contingency elements. The framework's tenets are based on contingency management and the integration of information security policy, risk management, internal control, and information auditing theories to develop an information security architecture that is coherent with organizational objectives (Hong et al., 2003). My goal was to expand on and highlight different perspectives regarding security, risk management, safety, and overall satellite cradle-to-grave management.

Definition of Terms

Kessler syndrome: A predicted phenomenon that may occur if multiple satellites and pieces of space debris start crashing into each other. The result would be space debris creating even more debris, which could cut communications and limit future space travel (Torky et al., 2019).

LEO: The lowest possible range for orbit that satellites can dwell in, and most satellites reside here (Bai et al., 2021).

Satellite hacking: The action of non-state actors, nation-state actors, insider threats, or lone wolves to gain unauthorized or unsanctioned access to IT functions aboard satellites (La Bella, 2021).

Space debris: Remnants of space launches, nonfunctioning satellites, and pieces of materials released from space collisions (Olivieri & Francesconi, 2020)

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are facts that are considered to be accurate but require verification through research (Theofanidis & Fountouki, 2019). In this study, I made several assumptions. The first was that I assumed that since the participants already worked in the space industry, they may have already been very familiar with the Kessler syndrome phenomenon and methods to decommission satellites. The second assumption was that participants routinely trained for worst-case scenario days of potential satellite collisions.

Limitations

Limitations are a study's potential weaknesses that are identified prior to conducting research (Babchuk, 2019). It was crucial to identify the limitations of a study ahead of time and plan accordingly. Some limitations of the current study were that interviews needed to be conducted remotely through the Zoom platform due to the COVID-19 pandemic concerns. All interviews were conducted remotely and only voice was recorded for transcription. Some topics may be considered sensitive data, and only unclassified documents could be used. The sample size of this study was affected because I could not interview active-duty military or discuss classified information.

Delimitations

Delimitations can be summarized as anticipated factors that could play a role in how the results of a study are interpreted (Sampson et al., 2014). The scope of this study was space assets and trash orbiting in LEO; however, high Earth orbit and medium Earth orbit were also explained and explored in the study. The boundaries of the study included declassified strategies in LEO to remain within the parameters within this study.

Significance of the Study

Contribution to IT Practice

This study is significant because there is an IT problem associated with satellite issues and how future communications may be affected if satellites are hacked, crash, or become unresponsive. My goal was to promote more awareness on decommissioning satellites in LEO. In 2019, NASA reported more than 500,000 pieces of debris were orbiting the Earth and that this number would continue to grow (Migaud, 2020). Satellites are not self-healing, and repairs can be expensive, which is why preventing collisions is essential. Large orbiting space objects, also known as debris, could initiate the fragmentation of a significant part of a satellite (Olivieri & Francesconi, 2020). Satellites can also be hacked by adversaries, potentially turning them into weaponized projectiles (Van Camp & Peeters, 2022). News coverage seems to focus on new deployments of satellites, but more attention could be placed on satellites being removed without creating more space junk (Mullick et al., 2019).

The results of this study can contribute significantly to increasing awareness of the different perspectives and strategies that can be used to decommission LEO satellites

without affecting Kessler syndrome. Furthermore, innovations shared and explored in the current study may be adopted by agencies across the space industry to declutter space and protect satellites from cyberattacks (see Brewer et al., 2022; Z. Hou et al., 2022). Implications for positive social change may include the entire space industry and not just one organization, such as NASA. NASA is not the only player in the space industry, although some may believe they control all space operations. There are many agencies and nations that affect satellites and space operations. Change may not always be easy, but it can be essential when considering continuous process improvement. A strategy can be sufficient for years but then become obsolete as an issue evolves. I hope that this study reaches the desks of satellite engineers and leaders in the space industry to help them understand the importance of analyzing the strategies they are using to decommission satellites in LEO. LEO was a crucial section to focus on because it is where the International Space Station (ISS), which is occupied by astronauts from various nations, forbits around 250 miles from Earth (Hassan & Davenport, 2022). Various components of the ISS have been built to withstand minor impacts from debris, but more significant impacts in sensitive or unprotected areas could present dangerous situations (Shaker et al., 2021). The ISS is subject to more than just space debris; it is also affected by ionizing radiation, temperature extremes, meteoroids, ionospheric plasma, and ultraviolet radiation (Shaker et al., 2021). Spare parts are minimal on the ISS due to lack of storage space, and resupplies are scheduled every 2 to 3 months (Shaker et al., 2021). Any damage to the ISS places the lives of the astronauts and cosmonauts in danger, but space debris tracking decreases the risk of potential collisions in LEO (Shaker et al., 2021).

Implications for Social Change

Social change should be considered in how the space industry contemplates the decommissioning of LEO satellites in the future so humans may have continued space travel and satellite-fueled communications. One satellite accident or failed return to the atmosphere for destruction may create a chain reaction causing massive communication outages (Meng et al., 2021). One nation might accidentally or intentionally damage another nation's satellite, which could start the chain reaction and multiplication of space debris. No country is designated to police space, and space is shared amongst several nations and the entire space industry. The average citizen in any nation may have some fear of being struck by falling space debris (Hassan & Davenport, 2022).

A Review of the Professional and Academic Literature

In this study, I explored strategies used by IT satellite managers in the space industry to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. The literature review includes studies on how LEO satellite collisions and cyberattacks could affect all humans who rely on satellites for their operations. The literature review is a combination of peer-reviewed, academic journal articles; internal organizational documents, such as doctrine; and publicly released strategies and innovations to de-orbit satellites found in Google Scholar and databases accessible through the Walden University Library. I also conducted internet searches across government, military, and space agency websites to gather literature about current practices, remedial guidance, reports, and innovations. Personal forums and .org websites were excluded from the study because of their potential lack of credibility.

I used the following keywords to search for appropriate literature: *Kessler Syndrome, satellites, space, Space Force, telecommunications, space debris, space trash, space junk, satellite hacking, global positioning system, satellite communication threats, orbit, reusable rockets, reusable space technologies, space nets,* and *space magnets.* Additionally, I carried out searches with similar combinations of these selected keywords to find data related to the study. The sources provided academic perspectives about satellite technologies. Table 1 displays information regarding selected peer-reviewed articles, non-peer-reviewed articles, books, and webpages.

Table 1

Details of Literature Reviewed by Year of Publication

	Older than 5 years	2018	2019	2020	2021	2022	2023
Peer reviewed	30	4	30	36	30	41	12
Non-peer reviewed	0	0	0	0	2	1	0
Books	2	0	1	3	2	1	0
Webpages	7	0	6	4	3	5	1
Total	39	4	37	43	37	48	13

There are three main parts of this literature review: (a) supporting and opposing arguments for the conceptual framework, (b) synthesis and analysis of emerging themes discovered in the literature, and (c) a synthesis of previous research about decommissioning satellites out of orbit. In the literature review, I describe the creation and justification behind the conceptual framework of the ISTISM and its application to

rapidly decommissioning satellites out of LEO. Some of these areas include integrating information security policies, risk management, internal controls, and information auditing. When these areas overlap, they allow for the potential prediction of management outcomes. Within the subsection on ISTISM, I also discuss how strategies were used to rapidly decommission satellites from LEO that may have been targets of cyberattacks or damaged for other reasons. Most of the more than 60 sources included in the literature review are scholarly and peer reviewed and were recently published within the last 3 years.

ISTISM

Applying a proper comprehensive framework can assist organizations in achieving objectives through running through integrated components. ISTISM is a popular framework used by academia and practitioners to conduct empirical research and application (Hong et al., 2003). The complexity of protecting space assets and the different approaches within ISTISM allows for researchers to use the framework, which was proposed by Hong et al. (2003), as the foundation for addressing a specific research problem. Selecting a sufficient framework is crucial for a researcher to dive deeply into solving a problem (Savin-Baden & Major, 2023). Applying the ISTISM framework provided a strong foundation for addressing the specific research problem in this study because the ISTISM emphasizes integrating diverse security measures, policies, and protocols into a cohesive system, nurturing a robust and harmonious environment for information security.

The ISTISM was created through the merging of five theories: (a) security policy theory, (b) risk management theory, (c) control and auditing theory, (d) management system theory, and (e) contingency theory (Hong et al., 2003). Although the ISTISM is quite extensive, it offers robust and meticulous benefits towards an organization wishing to secure IT assets (Eloff & von Solms, 2000). The ISTISM allows users to consider the numerous components of security management and mix them into a unified system, which may lead to enhanced security, risk management, and overall organizational resilience.

Performing the literature review and data analysis through an ISTISM lens allowed me to better understand current factors that contribute to vulnerabilities and exploitations targeted at space assets along with analyzing strategies to protect and remove IT satellites from LEO if targeted by cyberattacks. Using only one or two of the five core theories within the ITISM would limit the overall scope of the study and prevent an understanding of the complexities involved with the research problem under review (see Hong et al., 2003).

A primary driving factor behind the ISTISM framework is a focus on risk management. Risk management under the ISTISM framework addresses the interactions between subsystems and their collaboration with external factors (Ajupov et al., 2019). The principal objective of risk management is to decide which security controls are required to keep the security risks at an acceptable level; this is completed by assessing organizational assets, related threats, and vulnerabilities (Hong et al., 2003). The ISTISM is adequate for realizing information security management needs, describing information

security management strategies, and predicting management outcomes (Hong et al., 2003). Although all outcomes may not be 100% predictable, planning for worst case scenario days may showcase gaps in strategies. Security management strategies should consider infrastructure, policy, and risk assessment compliance and programs (Georgiadou et al., 2022). In the ISTISM, Hong et al. (2023) explained that information security is not just a technical issue but also addresses business concerns that require engagement from all levels of an organization or agency.

The security policy theory portion of the ISTISM, in association with strategies IT satellite managers use to decommission satellites out of LEO if targeted by cyberattacks, can be used to directly secure national interests and humans on Earth. Security architecture must be dependable within an organization to meet objectives. Haphazard or weak security policies can lead to potentially dangerous situations in LEO (Boley & Byers, 2021; Lalbakhsh et al., 2022). IT satellites and their connecting networks must have survivability when operating in LEO (H. Li et al., 2022). Correctly identifying weaknesses and gaps will allow decision-makers to see areas of concern and develop solutions to combat risks. Risk cannot be avoided 100% due to human nature, natural disasters, or freak accidents (Stein et al., 2019). The security policy portion of the ISTISM focuses on assessing problems and persuading top management to form, draft, implement, and maintain policies (Kabay, 1996). IT satellites are vulnerable to malicious cyberattacks and can be affected by internal or external attacks (T. Li et al., 2019). Uncovering best practices and strategies used by IT satellite manufacturers and managers may directly contribute to securing space assets.

In 1961, the Committee on the Peaceful Uses of Outer Space was created by the United Nations to increase the amount of information shared regarding space assets launched (Migaud, 2020). There is a need for international and global policies related to limiting the amount of space debris (Mohanty, 2021). Creating solutions will be difficult because the government, military, and civilian sector organizations launch assets into space (Mohanty, 2021). Some nations are new to space operations and may not track what other nations do with their existing space assets (Meng et al., 2019).

Since 1965, 89% of all objects launched into space have been registered with the United Nations Office of Outer Space Affairs UNOOSA Space Object Register SOR to comply with Committee on the Peaceful Uses of Outer Space (Marboe, 2019). The Outer Space Treaty was created in 1967 and mentioned national activities in outer space, but it needs to be clarified and is seen as outdated today (Dilworth & Osborne, 2022). The Outer Space Treaty has several provisions and states' responsibilities through licensing regulations, statutes, oversight of launches, on-orbit activity, and other space-related conduct (Dilworth & Osborne, 2022). The Outer Space Treaty of 1967 was opened for signature by the three depository governments, which were Russia, the United Kingdom, and the United States (Gupta & Rathore, 2019). The Outer Space Treaty includes the Moon, satellites, and other celestial bodies in space (Dilworth & Osborne, 2022). Failure to revise and educate all nations currently in the space race could result in many abandoned or littered satellites in orbit, which may contribute to Kessler syndrome (Muñoz-Patchen, 2018). International and domestic laws are hard to enforce because there is no true space police force that ultimately has jurisdiction over Earth's orbit

(Dilworth & Osborne, 2022). Littered satellites pose a significant issue to future space travel and increase the potential of collisions between active and inactive space objects.

Many end users rely on mobile devices to check weather, directions, and news updates. Without satellites, these services could be degraded or nonexistent. Although the number of satellites is increasing the quality of life for humans, their existence may spark a phenomenon known as the Kessler syndrome, which is a theory that one collision in space with satellites or other space junk would ignite a chain reaction of crashes. NASA scientist, Donald J. Kessler, established NASA's Orbital Debris Program Office in 1979, from which the scientist researched the topic of satellite collisions in LEO until retiring in 1996 (Dunstan, 2013). A tiny fragment of metal or paint chip colliding with a satellite could knock out its ability to operate (Kawamoto et al., 2020).

Although space is ample, with miles of open space above the atmosphere, space debris has become an issue (Mullick et al., 2019). Most satellites operate in LEO, defined as 200 to 700 km above the Earth's surface (Sowell & Taheri, 2022). Some satellites can even be seen without the assistance of telescopes or binoculars. Recently, satellites have been designed to use their last amount of fuel to reenter Earth's atmosphere to burn up safely (Tomizaki et al., 2021). LEO has about 75% of all artificial trackable objects orbiting the planet, which places much responsibility on the Orbital Debris Program Office and hinders planning for future space launches (Migaud, 2020).

The Orbital Debris Mitigation Standard Practice (ODMSP) was created by the United States in 2001 and states that any spacecraft or satellite in LEO must limit postmission disposal to 25 years after the end of mission operation (Migaud, 2020).

ODMSP is broken down into four pillars with specific actions belonging to assigned federal entities. The pillars fall into the three categories of prevention, mitigation, and defense, which aim to minimize the total amount of space debris and secure future space operations. According to Migaud (2020), in ODMSP Pillars 1 and 2, the following specific actions are assigned to the following federal entities:

- Federal Aviation Administration:
  - Approve all launch attempts.
  - Approve all reentry into the United States.
  - Regulates contents and structure of reusable and expendable rockets.
  - Reviews risk assessments of launch, operational lifetime, and reentry.
- Federal Communications Commission (FCC)
  - Approve all telecommunication satellites.
  - Sets restrictions on assets size and dimensions.
  - Set restrictions on radio frequencies used during orbit
- NASA
  - Approve all launches using U.S. public space infrastructure.
  - Oversees debris assessment reports.
- National Oceanic and Atmospheric Administration (NOAA)
  - Approve all space-based remote sensing assets.
  - Collects projected orbital path and all technology aboard assets.

In ODMSP Pillar 3, Migaud described the assigned actions as:

- FCC

    - Regulates asset maneuvers and orbital patterns when movement is necessary.
- NASA
    - Situational awareness of space.
    - Controls collision avoidance measures aboard ISS.
    - Carry out high velocity impact research projects.
- Department of Defense
    - Situational awareness of space.
    - Share satellite positioning data with various nations.
    - Provide 72-hour advance notification warning of potential collision to satellite operators.

In ODMSP Pillar 4, the actions are:

- Department of Defense
    - Research active debris removal technologies.
- NASA
    - Mandates assets must exit orbit within 25 years of launch.
    - Gather asset/satellite retirement plans.
- FCC
    - Collect the operator's asset retirement satellite plans (Migaud, 2020).

Contingency management is crucial to integrating information security policy, risk management, internal control, and information auditing theories to form an information security architecture consistent with organizational objectives (Hong et al.,

2003). Data collected and shared from satellites varies depending on the engineered reason. The logical connections between the ISTISM framework and the nature of the current study included the need to understand strategies used by space agencies to decommission satellites without the effect of Kessler syndrome. Space agencies across the globe face a similar issue when it comes to protecting satellites and other spacecraft from space debris. IT satellites and other technology-based space probes must be protected from space debris or adversaries aiming to cause malicious acts (Lucas et al., 2020).

Multiple studies have been carried out with a primary focus targeted at satellite collisions causing more space debris due to increased space launches from various organizations and countries (Raguraman et al., 2020). More studies about satellite hacking and weaponizing space objects are coming to light (Bateman, 2022). Anti-Satellite (ASAT) weapons could be launched by adversaries to attack foreign satellites with the intention of destruction or interference (Bateman, 2022). Attacks are being configured and dispatched targeted at satellite operator maneuvers by hacking signals to the satellite, which changes a satellite's physical location in order (Dilworth & Osborne, 2022). When the two issues are overlapped, it illustrates that hacked satellites can become space debris if owners cannot regain control. One satellite accident or a failed return to the graveyard orbit for destruction may create a chain reaction causing massive communication outages (Dilworth & Osborne, 2022). Furthermore, one nation might accidentally or intentionally damage another nation's satellite, which could start the chain reaction and multiplication of space debris (Dilworth & Osborne, 2022). An accidental or

intentional situation where satellites collide could be detrimental to space operations for all nations (Bateman, 2022).

The risk management theory portion in association with strategies IT Satellite Managers use to decommission satellites out of LEO if targeted by cyberattacks can limit the potential of risks while allowing decision-makers to plan for worst-case scenarios. Manufacturing and protecting IT satellites from cyberattacks is essential when bearing in mind the risk management needed to protect space resources. The end goal of risk management within an organization is to make IT security risk at an acceptable level (Tohidi, 2011).

Each orbit has its purpose and commonly deployed satellites residing within them. Some satellites stay in a fixed orbit to monitor their target consistently while others move about. Having numerous satellites in multiple orbits increases the potential for collisions. Just because space is vast, there is a large concentration of expended, broken, or in-operable artificial assets stuck in the LEO (Morin & Richard, 2021). Although space is vast, the immediate area around the Earth could become overcrowded or dangerous because of the large number of orbiting satellites and debris. Depending on the purpose and engineering of the satellite dictate what orbit it needs to reside in to complete its purpose. Some satellites may only operate correctly or respond to commands if they end up in the right orbit. The Geostationary Orbit (GSO), sometimes referred to as Geosynchronous Orbit (GSO) stays in orbit around the equator, which makes tracking the satellite easier, but other satellites may not stay in the exact line while in orbit. Real-time tracking is essential to keeping satellites and human-crewed stations safe from debris

collisions (Bianchi et al., 2022). The Bi-static Radar for LEO Survey can monitor debris fragments and their re-entry resulting in collision avoidance (Bianchi et al., 2022). Preventing collisions is not a job for only one nation to bear because all the nations deploying satellites into LEO may be contributing to space debris or increasing the chances of a collision unleashing the Kessler Syndrome phenomenon (Bianchi et al., 2022).

Each satellite must be engineered, configured, and launched properly into its respective orbit (Mohan & Kishore, 2021). Newer satellites have built-in protection systems and could also be covered in nets that capture fragments of debris prior to being struck Olivieri & Francesconi, 2020) The growing amount of space debris has altered the way communication satellites are engineered to increase their longevity. A satellite that slips into the wrong orbit may not have enough fuel or the technologies to return to its predicted position (Krajcovic et al., 2020). Artificial satellites require expensive alterations to ensure they can operate in the harsh space environment (Runnels, 2023). Communication satellites must be modernized for the potential collisions with debris in LEO (Adushkin et al., 2020). A lot of observation and real-time tracking is needed to focus on unresponsive space debris objects to prevent collisions with functioning satellites (Eriksson & Giacomello, 2022). Old unneeded satellites still in orbit are dangerous since they may be on the same orbital plane as functioning devices (Krajcovic et al., 2020). Satellite operators may have enough fuel and time to adjust positioning for functioning devices, but broken assets are dangerous projectiles (Egeli, 2021).

It takes multiple months and years for a planning team to fabricate and construct a satellite for launch, and failure to protect the asset could result in a significant financial loss (Lian et al., 2022). If a satellite is damaged during transportation, launch, or in orbit, it generates a review of what caused the mishap. The findings of the mishaps could be used to deter future losses and identify the party at fault. Accidents due to human error or natural disasters happen, and space agencies must accept the potential risks associated with deploying satellites into orbit. Communicating lessons learned across various space agencies may benefit the entire globe and future space travel for everyone. Future launches could be hindered or scrubbed during launch windows because of too much debris passing the telemetry path (Migaud, 2020).

The integration of control and auditing theory with the strategies employed by IT satellite managers for decommissioning satellites in LEO, especially in response to cyber-attacks, has the potential to reveal previously unaddressed gaps or areas of concern. As humanity's interest in space exploration and expansion grows, there is a corresponding need to prioritize the auditing of technologies and policies in emerging space domains (Alewine, 2020). Regularly reviewing controls and processes associated with satellite manufacturing and operation is crucial for proactively identifying vulnerabilities before they can be exploited (Dilworth & Osborne, 2022). Conducting audits of control systems, policies, and IT systems utilized for satellite control on a frequent basis helps uncover vulnerabilities that could lead to compromises or loss of control (Kucklick & Müller, 2021). ISTISM places strong emphasis on ensuring compliance with pertinent laws, regulations, and industry standards. It not only encourages organizations to establish and

maintain a compliance framework but also stresses the importance of aligning it with the legal and regulatory requirements of their respective nation or international laws, as well as industry best practices (Hong et al., 2003).

The application of contingency theory and management system theory components of ISTISM in conjunction with the strategies employed by IT Satellite Managers for decommissioning and protecting satellites in LEO when faced with cyber-attacks, can potentially provide insights into addressing the challenges posed by the Kessler Syndrome phenomenon. ISTISM fosters a culture of continuous improvement in information security (Hong et al., 2003). ISTISM involves regular evaluations of the effectiveness of security measures, identification of areas for enhancement, and timely implementation of necessary changes to safeguard assets. This iterative approach ensures that security measures remain current and responsive to the ever-evolving threats in order to maintain the protection of assets. ISTISM underscores the criticality of raising awareness and delivering comprehensive training to employees concerning information security. This is because the actions of a single employee, whether intentional or inadvertent, with poor IT security practices, can have far-reaching consequences for the entire organization (Ignatovski, 2021). Space Doctrine Publication (SDP) 1-0 highlights that Space Force members are embedded with the National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGA), National Air and Space Intelligence Center (NASIC), the Department of Commerce, and NASA. The integration assists in protecting commercial, government, and military satellites, launch complexes, and system support systems (SDP, 2022). The Space Force was created as the sixth

military branch, with their primary focus being intelligence, cyber, and space operations (Bowers, 2022). The Outer Space Treaty of 1967 did not consider cyber operations as part of the provisions when originally created (Dilworth & Osborne, 2022).

Training and application of Defensive Cyber Operations (DCO) are crucial to safeguarding communication satellites that could be hacked by adversaries (Crane, 2018). It is vital to expand DCO capabilities in space because the Department of Defense sees the demand for satellite connectivity proliferate across civilian and military sectors. Many end-users require some type of connection for devices in their homes, and the satellites used to obtain the signal require protection (Shinn, 2022). The protection of satellites focuses on end-users in their homes and encompasses military operations such as vehicles, aircraft, or sea vessels needing satellite connectivity. Currently, more than 3 billion internet users rely heavily on IT satellite communications (Yang, 2020).

Supporting Theories Regarding the Conceptual Framework

Supporting theories provide a foundation for the development of the conceptual framework used in the study. Supporting theories support the researchers understand existing knowledge, concepts, and the relationships related to the phenomenon under research. In qualitative research, the use of supporting theories improves the credibility and trustworthiness of the study (Cloutier & Ravasi, 2021).

Knowledge-based theory (KBT) focuses on the utilization of knowledge within an organization to create values through input-to-output transformation (Grant, 1996). KBT analyzes the strategies and resources of any organization to amplify performance (Jambak, 2015). The conflict theory was created by Karl Marx and highlights that

a society is in a state of perpetual conflict due to the competition for limited resources (Kasi & Sallah, 2021). The conflict theory of war stems from cumulative and growing conflict(s) between individuals, groups, and entire societies (Simon, 2016). Moreover, the conflict theory underscores the role of power efforts between different groups in shaping society (Bartos & Wehr, 2002). Practice-based view (PBV) theory is a revised form of the resource-based view (RBV) theory (Bromiley & Rau, 2016). PBV indicates exploring activities or set of actions that various organizations might execute (Carter et al., 2014). Capability-based view (CBV) theory allows an organization to measure their capabilities by analyzing the capability of rivals, competitors, or adversaries (Amiri et al., 2015).

ISTISM and KBT

ISTISM and KBT are similar because the goal is to create resources that can improve organizational performance later. However, the ISTISM theory focuses on securing information against threats. The KBT would also be a feasible alternative to gather information, and assets, expand collaboration and enhance overall decision-making (Guo et al., 2019).

It takes a large team to develop, transport, and launch a communications satellite into orbit. It will take a large team to properly decommission them from orbit without adding to Kessler Syndrome (Barato, 2022). Data has been generated to identify knowledge within space agencies to understand values through input-to-output transformations associated with methods to clear space debris. The RemoveDebris mission was the world's first Active Debris Removal (ADR) mission that produced

successful demonstrations in orbit (Aglietti et al., 2020). The primary tools used were nets, and harpoon captures to remove satellites and large enough pieces of debris from the LEO (Aglietti et al., 2020). On April 02nd, 2018, a satellite was launched to the ISS; on June 20th, 2018, it was redeployed using a NanoRacks Kaber system into an orbit of 251-mile LEO altitude (Aglietti et al., 2020). The ISS was chosen because the launch was part of the 14th Space X CRS (Commercial Resupply Service) to the ISS (Aglietti et al., 2020). Resupplying the ISS is challenging and requires extensive planning to ensure space debris is avoided and dodged at all costs. The team on the ground used various navigation techniques to align a harpoon capture to hit its target, resulting in a successful tether (Aglietti et al., 2020). The RemoveDebris mission ended with its final phase of disposing of debris through dragsail (Aglietti et al., 2020).

The SpaceX Starlink program plans to launch a total of 11,927 satellites across eight orbital planes dedicated to providing internet connectivity to 1 million user terminals on the Earth's surface (Xie et al., 2020). The famous space launch company SpaceX has received FCC approval to halve the orbital altitude of more than 1,500 future communications satellites to lower the risk of space debris and improve overall consumer latency (Brookin, 2019). The more satellites released into Earth's orbit increases the potential of collisions which could ultimately set off the Kessler Syndrome chain reaction. Innovations such as miniaturized satellites, also known as CubeSats, are being sent to LEO to provide communications (Chou et al., 2022; Cojocari et al., 2023). Nanosat Database CubeSat Unit (U) sizes vary such as (Y. Xie et al., 2020):

- 1U = 10 centimeters (cm) × 10 cm × 11.35 cm

- 2U = 10 cm × 10 cm × 22.70 cm
- 6U = 20 cm × 10 cm × 34.05 cm
- 12U = 20 cm × 20 cm × 34.05 cm

Computer-based studies have been carried out to predict CubeSat's contribution to the Kessler Syndrome phenomenon. Even though CubeSats are small and the inter-satellite distances are comparatively large, there will always be a concern for collisions in Space (Schafer et al., 2021; Xie et al., 2020). The assets orbiting space, the more likely collision is probable. CubeSat's computer-based simulation discovered that CubeSats would have a lower collision probability when compared to traditional-sized satellites but still may contribute to space collisions because of orbital plane drifting (Xie et al., 2020).

ISTISM is a better fit for my study since uncovering strategies to secure satellites against physical and digital threats is the end goal. The strategies uncovered in the study may aid future space agency professionals with predicting management outcomes. The five theories used to construct the integrated theory allow for a deep analysis of the problem it is applied to (Hong et al., 2003).

ISTISM and Conflict Theory

ISTISM and conflict theory are on opposite ends of the spectrum but complement each other. Suppose conflict is bound to happen due to the competition for resources, such as limited orbital planes from Kessler syndrome. In that case, ISTISM can be employed by a nation or space agency wishing to secure existing assets or future devices from compromise. The conflict theory states that a society will be in a state of perpetual conflict due to the competition for limited resources (Le Billon, 2001). When conflict

theory is applied to protecting space assets, it can highlight the inherent power dynamics and competition that exist in the realm of space exploration and utilization. Although space is vast, there is still existing competition for the deployment and safeguarding of IT satellites within LEO (Ren et al., 2021). Conflict theory recognizes that protecting space assets involves power struggles among different actors (Harrison et al., 2020). Nations around the globe may continue to have conflicts that extend from the ground, sea, and air into space causing IT satellites to become vulnerable to intentional or unintentional kinetic and nonkinetic attacks (Falco, 2020). Governments, military and private companies may compete for orbital real estate, assigned radio frequencies, and the sole use of specific space infrastructure (Ren et al., 2021).

Due to unrelenting conflict, ISTISM fits the need to tackle IT satellite cyberattacks that could lead to compromise. Preventing satellite cyberattacks may directly contribute to the determent of satellite collisions. Conflict theory highlights the unequal distribution of resources and capabilities among different actors in space. More technologically advanced and financially capable organizations or nations may have a substantial advantage in defending their assets such as space tools when compared to less developed or economically weaker organizations or nations (Adeyeye, 2020). Inequality may influence security concerns, as weaker actors may identify their assets as vulnerable to exploitation or aggression by more powerful entities.

The space race began in 1955 when tensions between the United States and Russia were high (Dawson & Dawson, 2018). The United States and Russia were considered world superpowers with the ambition of completing space missions (Trevino,

2021). The dangers of space were not entirely known, and the problem of space trash was likely not a topic of discussion. As technology advanced, so did the way humans communicate, broadcast, and collect valuable information, such as weather forecasts. However, the advancements in space had pros and cons because conflicting countries placed a severe interest in what another country was doing in space (Dilworth & Osborne, 2022). Sputnik 1 was the first artificial satellite launched into Earth's orbit by the Soviet Union on 4 October 1957 and was only 23 inches in diameter (Burns & Turchak, 2007). Weaponizing space was a concern because the lives and systems used on Earth could be affected (Van Camp & Peeters, 2022). Destroying or altering another country's space assets would not only hinder their communication but also cause a potential domino effect of future collisions. The Department of Defense and NASA use Space Surveillance Network (SSN) sensors to track 27,000 pieces of artificial objects that remain in space that no longer serve a beneficial purpose(s) (Kawamoto et al., 2020). Having the ability to track space debris is crucial so space professionals can predict potential collisions. The data collected from the SSN is used for several studies and computer-based simulators. As space operations continue, the number of pieces may fluctuate due to the creation of new debris or older debris burning up due to atmospheric re-entry. The cost of launching rockets also cuts back the charge for having a satellite (s) placed in orbit by a commercial company (C. Wang & Song, 2019). The more rockets that are launched increases the potential for more space debris (C. Wang & Song, 2019).

The term satellite is not reserved solely for artificial objects but encompasses all objects that orbit around an object larger than itself (Wall, 2017). The human population

most likely knows the term satellite as the artificial objects used for weather tracking, communications, and military operations. Movies and television shows have created scenes of satellites being hijacked or destroyed which may contribute to the viewer's perception of satellites. Movies and television depictions should not be confused with actual satellite operations because some actions are exaggerated. Commercial companies and news outlets may have altered how humans think of satellites. The human race has become familiar with satellites as manufactured machines that orbit the Earth in one of the following orbits (Riebeek & Simmon, 2009; Trishchenko et al., 2019):

Orbits

There are several common orbits which are varying miles from Earth's surface including (Riebeek & Simmon, 2009).

- LEO 111.8 – 1242.7 miles
- Polar/Sun-synchronous orbit 370–500 miles
- Medium Earth orbit 1242.7 – 22,232.6 miles
- Geostationary orbit 22,300 miles
- Geo transfer orbit 22,236 miles
- Highly elliptical orbit 22,232.6 + miles
- Burial orbit (Graveyard orbit) 22,400 miles

Typical satellites, their function, and residing orbit (Luu & Hastings, 2021):

- Communication Satellites
    - Relay and amplify radio frequencies (Television, radio, telephone transmissions)

  - Reside in LEO and GSO
- Navigational Satellite
  - Pinpoints user's position and improves travel on land and in the air
  - Reside in MEO
- Killer Satellites (Anti-satellite weapons (ASAT))
  - Space weapons engineered to incapacitate or destroy satellites for strategic or tactical purposes
  - Reside in LEO
- Miniaturized Satellites (CubeSats)
  - Used for communication purposes
  - Reside in LEO
- Recovery Satellites
  - Space debris mitigation tools
  - Reside in LEO
- Tether Satellites
  - Satellites or space craft connected together by strong cables used to generate electrical energy for fuel-efficiency
  - Reside in LEO
- Space Stations
  - A spacecraft created to support human crews
  - Reside in LEO

LEO satellites have drawn vast awareness and research since they have low latency, a large capacity and are easily deployable (Lian et al., 2022). Satellites are not self-healing, and repairs could be expensive, which is why avoiding collisions is significant. A broken satellite in orbit may require a specially designed repair satellite to tether to it to repair it or pull out of orbit (Migaud, 2020). More famous satellites, such as the Hubble telescope or the James Webb Space Telescope (JWST), could require human-crewed space operations to have trained astronauts physically repair or upgrade parts. Remote Piloted Aircraft (RPA) technologies have bled over to applying the concept to spacecraft (Koga & Fukui, 2022). Having a remotely piloted spacecraft removes the danger of placing a human in danger but still adds to the potential cluttering of orbits. SpaceX is developing methods to refuel and restock space objects with robotic refueling (Krenn et al., 2019). Research innovations are being targeted at employing space travel capabilities and rockets' reuse to deter space debris and advance space transportation (W. Feng et al., 2020).

Space debris is a growing problem and innovations are needed to remedy space debris before it jeopardizes future space travel and damages current space assets (W. Feng et al., 2020). Using robotic technologies removes the potential for human casualties and revolutionizes the way space junk can be removed safely and deliberately. Deploying satellites is becoming less expensive and happening more often with innovations such as rideshare aboard reusable rockets. With more launches, there should be a shift towards removing outdated communication satellites as new ones enter orbit. RPAs in space are also referred to as Free-flying space robots and chasers which do not feel the fatigue

humans would face in space (Koga & Fukui, 2022). Deploying Artificial Intelligence (AI) computing into space transportation for quick decisions and adaptive control for repeated flights may allow for space operations to be cheaper, faster, and more mobile while amplifying reliability (W. Feng et al., 2020). Using free-flying space robots multiple times before their return to Earth's atmosphere would reduce the amount of space debris and potentially become a process to declutter LEO (Koga & Fukui, 2022). The free-flying space robot's removal process comprises two steps: capture and drop (Koga & Fukui, 2022). The robot contacts the target debris using a manipulator in the capture step (Koga & Fukui, 2022). The drop step completes when the chaser forces the trapped target to sling it back into Earth's atmosphere (Koga & Fukui, 2022). The Free-flying space robot and operating crew must ensure the safety of the surrounding satellites to deter collisions and avoid contributing to the Kessler syndrome phenomenon (Koga & Fukui, 2022).

Start-up companies or established organizations can pay a fee, along with others, to have their satellites released into orbit (Falduto & Peeters, 2022). This allows companies and organizations with enough money to have their space assets lifted for a fee. On 11 December 2022, SpaceX launched the first private Japanese lunar landing mission aboard a Falcon 9 rocket valued at 67 million dollars (Industry doc, 2023). Orbital space debris is a negative aspect associated with the launch of spacecraft and satellites into LEO (Morin & Richard, 2021). The need to address the space pollution problem is essential if humankind wishes to carry on or expand the day-to-day technologies used, such GPS, communications, and weather tracking (Morin & Richard,

2021). Italy, Switzerland, and the United States are currently conducting campaigns to monitor space debris (Morin & Richard, 2021). In order to extend the sustainability of LEO, mitigation efforts must be enacted to reduce the creation of new debris; advancements in monitoring capabilities are needed to track even the most minor debris, and there need to be remediation initiatives to remove existing debris (Morin & Richard, 2021). Commercial companies are not restricted to a limited number of launches which allows the number of startup satellites deployed (Morin & Richard, 2021; Y. Zhou et al., 2022).

Iridium telecommunications may be considered well-known due to the many communication satellites currently in orbit. Iridium telecommunications satellites orbit around 480 miles from the Earth's surface (Tan et al., 2019). As of October 2020, 73 previously functioning Iridium satellites are now non-operational or no longer exist due to returning to Earth's atmosphere for re-entry burn (Sladen, 2020). Removing non-operational satellites is a problem that requires solutions before a massive chain reaction is set into action. Communication satellites are being engineered to last longer in orbit when compared to prior technologies. No set number of satellites is allowed in space, so no specific policy or guidance limits the number of objects in orbit; only US guidelines remove them after 25 years (Kopeć, 2018; Migaud, 2020). Countries around the globe also launch communication satellites to increase communications, weather capabilities, and government operations.

Primary launch organizations on Florida's space coast are NASA, SpaceX, United Launch Alliance (ULA), and Blue Origin. On December 28th, 2022, SpaceX launched a

reusable Falcon 9 rocket for the 172nd time and deployed 114 Starlink payloads valued at 67 million dollars (Industry doc, 2023). Using reusable rockets cuts the cost of launching payloads into orbit and lowers the risk of larger fuel tanks being left behind. Although more oversized items are being returned to Earth after a launch, more satellites are being deployed into orbit because of ride-share demand. SpaceX impresses sky gazers as they set records for rocket launches that place clusters of communication satellites into LEO (Groh, 2022). A Delta IV was developed by ULA which has a common booster core (CBC) that is 16.7 feet (ft) in diameter and 133.9 ft long (Krajcovic et al., 2020). This exact object is being tracked as space debris and could cause much damage in LEO if it collides with operational or nonoperational communication, GPS, or weather satellites (Krajcovic et al., 2020). According to Nudelman & Orwig, 2015, historical satellites have various sizes and purposes:

- Sputnik1
  - 2 ft
  - Launched 4 October 1957
  - Conducts atmosphere density testing
- NASA's Mars Reconnaissance Orbiter
  - 4.9 ft
  - Launched 10 March 2006
  - Conducts atmosphere and terrain testing
- Skylab
  - 86.3 ft

    - Launched 14 May 1973
    - Was the first United States space station
- Mir
    - 101.7 ft
    - Launched 20 February 1986
    - First Russian Space Station
- International Space Station
    - 357.5 ft
    - Launched 20 November 1998
    - Acts as a vessel for long-term exploration of space

There is a need to think of potential failed thrust contingencies and existing satellites in LEO past their life cycle (Sowell & Taheri, 2022; R. Wang et al., 2020). Some nations are just now entering the space race and launching space technologies, while others are purposely testing ways to destroy satellites (Sankaran, 2022). When these satellites are destroyed, they add to the space debris dilemma. Even though blowing up or hacking another satellite could be used as a military tactic, it ultimately places all other satellites in harm's way. No current sensor systems are designed to track tiny space debris particles that can still cause damage to rockets, satellites, and spacecraft (Raguraman et al., 2020). A majority of the countries responsible for a majority of the present debris in space are the United States, Russia, and China (Raguraman et al., 2020). The larger the piece of debris in space, the larger the impact and the potential damage it could cause if it collides with a satellite or human-crewed station such as the ISS

(Raguraman et al., 2020). There are 7200 satellites in orbit with 4300 still operational which means that 2,900 nonoperational satellites in orbit require decommissioning before contributing to Kessler syndrome (Mohanty, 2021). De-junking Earth is another term for safely removing space debris from orbit without generating more pollution (Mohanty, 2021). There are nearly 34,000 artificial objects in space larger than 10 centimeters (cm), 900,000 objects ranging from 1-10cm, and 128 million objects in orbit measuring 1 millimeter (mm) to 1cm in size (Mohanty, 2021).

There is increased attention on satellite-to-satellite cyber-attacks which requires the need to propose new defenses and resilience techniques to ensure policies are sufficient to prevent IT satellites from being compromised via cyberattacks (Brewer et al., 2022; Falco, 2020). By understating the more complex sub-issues through ISTISM policymakers and stakeholders may navigate the complexities of space security, address potential conflicts of interest, and work towards more equitable and stable policies for protecting IT satellites from cyber threats.

ISTISM and PBV

ISTISM and PBV are similar because they identify specific techniques and implementation strategies to give an organization an advantage. Discovering the best practices and applying them could directly contribute to the success of an organization (Tian et al., 2023). PBV specifies the exploration activities or set of actions that various organizations may execute (Carter et al., 2014). PBV relies on collective practices and routines used to create and sustain competitive advantages for an organization(s) (Silva et al., 2022). PBV is often associated with supply chain management to plan for potential

shortfalls. PBV suggests that organizational success is not dependently reliant on resources or capabilities but considers individuals and groups within the targeted organization who mutually engage in activities and foster shared knowledge and routines (Tian et al., 2023).

Collective practices and routines can be exercises are carried out for IT professionals and amateur hackers to participate in satellite hacking challenges (United States Air Force USAF, 2020). Conducting hacking challenges allows space asset managers to uncover vulnerabilities for correction. Finding an issue with programming or hardware in a safe environment is better than discovering exploitations due to real-time failures in space. Exploitations discovered in one satellite may prove valuable to another satellite which has yet to be hardened to prevent specific vulnerabilities. Those participating in the satellite hacking challenges are in a controlled environment with Non-Disclosure Agreements (NDA) to prevent the findings from being shared or leaked to adversaries (Adeyeye, 2020). Organizations can conduct tabletop exercises, or computer-based simulations until the subsequent satellite collision occurs to practice communication flow and identify communication gaps (Xie et al., 2020).

PBV identifies the necessity for organizations to continuously advance and adapt their practices to meet shifting circumstances and evolving threats (Assumpção et al., 2023). Although PBV can be applied to organizations to develop robust and effective practices, by focusing on routines, and knowledge-sharing mechanisms, ISTISM may be a better framework to discover mitigation strategies for implementation to protect IT

satellites from cyber threats due it its complex and in-depth consideration of multiple IT governance, information security and control aspects.

ISTISM and CBV

ISTISM and CBV differ because organizations may not know the exact capabilities of their rivals, competitors, or adversaries. CBV is a strategic management framework that emphasizes the internal capabilities and resources of a competing organization to gain an advantage (Varadarajan, 2020). Although the exact capabilities may not be known, ISTISM can still be applied to protect security, improve organizational performance, and focus on protecting IT satellites from cyber threats. CBV theory can be used if predicted or assumed capabilities are applied if known capabilities are exhausted.

Through CBV a researcher can leverage the known and predicted cyber capabilities to produce effective results to protect IT satellites in LEO. This is because CBV theory considers risk assessment and continuous monitoring as critical components to cutting dangers. Risk management in the space domain is crucial because identifying and assessing potential risks may lower vulnerabilities associated with space assets. CBV theory incorporates investing in research, development, recruiting, and gathering highly skilled personnel, along with establishing partnerships with technology providers to ensure access to cutting-edge solutions (H. Zhang et al., 2019).

Other than kinetic attacks, satellites can be targeted through their communication connections (La Bella, 2021). War domains have moved from air, land, and sea to cyber and space fronts as adversary's research technologies to attack their enemies by attacking

communications satellites, ground stations, and other satellite control systems (Dilworth & Osborne, 2022). Communication satellites have become a primary source of stability for superpower nations such as the United States and Russia (Bateman, 2022; Haralambous et al., 2022). Satellites provide various human services on Earth, such as navigation, telecommunications, television, weather, science, and military operations (Ai et al., 2022). If these systems fail, the repercussions could be drastic to daily lives on Earth. Mass panic could become a reality if Kessler Syndrome or cyber-attacks disabled satellite communications. Communication satellites are heavily relied on by the human population, and issues with data collection, receivers, and command to satellite protocols place the object(s) in a potentially harmful situation (Cartis et al., 2021). Satellite components that direct software or hardware functions could fall victim or become compromised if not properly hardened, monitored, or protected (Tu et al., 2020). Satellite owners and operators must now consider countermeasures for kinetic kill vehicles, radiofrequency jammers, chemical sprayers, high-power microwaves, and robotic mechanisms (La Bella, 2021).

Cyber-attacks are ever evolving, which may require future consideration on how communication satellites and ground stations are configured to advert attacks. Iranian hackers breached the computers of the American satellite technology industry through the deployment of a fake website that was activated by an unsuspecting college professor (Rawnsley & Hughes, 2019). Cyber threats are targeted at cyberspace and space domains (Dilworth & Osborne, 2022). Outer space is not policed by one nation or organization, so discovering who deployed anti-satellite attacks is challenging (Manesh et al., 2019).

The rate of satellites being launched in LEO is increasing significantly, whereas the decay rate of orbital debris is still the same (Surdi, 2020). Blockchain technologies are a new strategy used in new satellites to act as tracking networks (Rabjerg et al., 2021; Surdi, 2020). Employing blockchain technologies for tracking purposes can expand the capabilities of tracking space debris. Using blockchain technologies would alleviate most of the tracking needed from ground stations and modernize how assets could be tracked in real time while in orbit (Surdi, 2020). Not only will blockchain technologies assist in identifying space debris, but they can also be used to manage traffic in space and increase awareness of the growing space pollution problem (Surdi, 2020).

ISTISM fits my study better because I am not requesting access to cutting-edge solutions firsthand due to their likely classification levels and require need to know requirements. After a successful ISTISM theory application, a follow-up CBV theory application can be deployed to build unique and difficult-to-replicate competencies, which may ensure the protection of space assets allowing space agencies to maintain a competitive advantage in the goal of protecting IT satellites from cyber threats.

Strategies to Remove Satellites From Orbit

Dragsail technologies are a potential solution to combatting a portion of the space debris problem. Dragsail slows down spacecraft, satellites, or other space debris, progressively reducing the altitude of its orbit until the craft burns in the Earth's atmosphere (Kuwahara et al., 2022). Using a sail to slow down an object in space is a viable option for decluttering space (Kuwahara et al., 2022). Large objects are still stuck in orbit, requiring assistance to safely de-orbit, and drag sails could directly contribute to

limiting the amount of space debris (Zander et al., 2023). If measures are not utilized, de-orbit out of date, or dead satellites, they may cause a chain reaction of crashes (Ailor, 2022). Using drag sails in parallel with sophisticated navigation and cameras, targets can be acquired, tethered, and then dragged into Earth's atmosphere for obliteration (Kuwahara et al., 2022). Drag sails are a safe alternative to chemical sprays, lasers, and incendiary technologies (Aglietti et al., 2020).

It is imperative to enhance the technologies required for avoiding collisions and properly disposing of new IT satellites (Falduto & Peeters, 2022). While newer satellites are being developed with cybersecurity measures, the challenge lies in fortifying existing satellites already in orbit (Han et al., 2020). Engineers are now exploring orbital defense controls and protective software and hardware for LEO satellites (Du et al., 2021). Recommendations can be made to improve satellite planning and engineering, ensuring their safe re-entry into Earth's atmosphere at the end of their operational life (Raguraman et al., 2020). Exceeding the expected lifespan of satellites risks leaving them stranded in space without fuel for controlled destruction (Bianchi et al., 2022). Some companies are implementing measures to reuse and recycle rocket parts, contributing to the prevention of future space debris (Sacchi et al., 2022). Advanced debris removal (ADR) methods encompass various reentry approaches such as controlled, non-controlled, expendable, reusable, demisable, and non-demisable systems (Barato, 2022). Controlled re-entry is favored as it enables space professionals to mitigate numerous risks (Barato, 2022).

Most communication satellites are engineered to use the final amount of fuel to re-enter Earth's atmosphere to burn up, while other satellites propel themselves far away

from Earth's gravitational pull (Huang et al., 2022). LOE satellites benefit by burning up in Earth's atmosphere because of their proximity, while satellites in further orbits push themselves outwards (Huang et al., 2022). A satellite from a distance orbit projecting itself toward the Earth may increase the chances of satellite collisions (Kawamoto et al., 2020). Satellites that re-enter through the atmosphere may not incinerate one hundred percent (Kawamoto et al., 2020). The remaining pieces of the satellite are calculated to land in a remote area in the South Pacific Ocean, known as the Spacecraft Cemetery (L. Fernandez et al., 2020; Häder, 2021). The Spacecraft Cemetery was selected because of its remote location and is one of the places on Earth with no close civilization (Häder, 2021). This action prevented space junk from staying in orbit and reduced the chance of debris landing in the human-populated area (Häder, 2021).

Although the graveyard orbit is used as a distance collection point, future space professionals may need to engineer a method to destroy a large number of operational satellites (Dilworth & Osborne, 2022). Collisions in the graveyard orbit could generate even more space debris that orbits the Earth, ultimately hindering future space missions. If enough pieces of debris start colliding and generating more debris, Earth may eventually be crowded by a net of space junk or rings similar to Saturn (S. Singh & Purbey, 2022).

In March 2019, India utilized an Anti-Satellite (ASAT) missile to obliterate one of their own satellites, which resulted in the generation of over 250 trackable pieces of debris (Migaud, 2020). As of 2022, there are 100 very large dead satellites and rocket stages orbiting in LEO, which presents a problem of potential collisions that could ignite

the Kessler Syndrome phenomenon (Ailor, 2022). Technologies and concepts exist to decommission and remove space debris from orbit. The concepts include lasers, nets, chemical spray, and magnetics (Raguraman et al., 2020). Lasers, nets, and chemical sprays can tackle large items, while magnetics may focus on large and small debris. Over 750,000 objects orbiting the Earth are calculated to be over the size of a coffee bean or 1 cm (Mark & Kamath, 2019). Ground-based lasers are a potential solution to safely deorbit satellites from LEO to lower the amount of space debris (Huang et al., 2022). Ground-based lasers can be employed to utilize a laser, ion beam, solar radiation, and other energy beams to interact with space debris to force it to move out of its orbit. Focusing lasers on satellites and space debris can slow down the object(s) enough to pull them into Earth's atmosphere for obliteration (Huang et al., 2022). Ground-based laser technology is a safer and less expensive alternative to launching tethered satellite vehicles to remove other satellites from orbit physically (Huang et al., 2022).

In 2019 Japan Aerospace Exploration Agency (JAXA) conducted a test with an electrodynamic tether named the Kounotouri Integrated Tether Experiment (KITE) which used stainless steel and aluminum wires to grab onto space debris in order to drag them down into lower orbit for incineration (Hori et al., 2019). However, it failed (Mark & Kamath, 2019). Although the technology failed, it is a step in the right direction to test it out again with modifications after applying the lessons learned. With these technologies, there is potential for many space applications to benefit from tethered satellites, such as propellantless propulsion, cargo transportation, orbital transfer, and debris removal (H. Li et al., 2022). Propellantless propulsion tactics utilize solar sails to move about in orbit

without fuel (X. Li et al., 2022). Applying propellantless propulsion to space debris removal saves money on fuel and aids in the goal of reducing the number of unused assets orbiting the Earth in LEO (H. Li et al., 2022).

The German Aerospace Center (DLR) has plans to test laser technology focused on locking onto space debris to evaporate the materials on the surface, which would slow it down enough to reenter Earth's atmosphere (Walker, 2019). Innovations to remove space debris and broken IT communication satellites are headed in the right direction but require testing (H. Li et al., 2022). Tensions between countries may rise, and space agencies from various countries test satellite removal because it may be seen as planning for future attacks.

Tethered Space Net Robot (TSNR) has been discussed as the most promising method to capture space debris or decommission satellites (Zhao et al., 2022). TSNR is classified as an Active Debris Removal (ADR) tool created to clear debris and abandoned satellites with a maneuverable tethered net within LEO (Zhu et al., 2022). Space-tethered satellite systems are advanced structures with large-scale and long-span attributes (X. Li et al., 2022). TSNR is engineered and configured to catch satellites and make them fall into Earth's orbit in a controlled matter without generating new space debris. ADR is necessary to remove items from orbit before the average orbital decay of 25 years. Computer-based simulations created by the European Space Agency (ESA) and NASA show a steady increase in space debris even under ideal conditions because there is an assumed collision rate of one every ten years (Schaus et al., 2021). Computer simulations are used to track trajectories and plan for potential mishaps (C. Wang & Song, 2019).

Since the 1950s, satellites have been launched into orbit on single use runs because they have been designed to use their last amount of fuel to reenter Earth's orbit for destruction (Redd, 2020). Northrop Grumman. They have created a Mission Extension Vehicle-1 (MEV-1) that can carry the fuel necessary to change a satellite's trajectory (Redd, 2020). This means older satellites stuck in orbit, needing fuel, may no longer be considered dead satellites or space debris if they can be refueled. MEV-1 can be compared to a jet pack or a tow truck, which maneuvers toward the targeted satellite and locks it on to deliver new fuel MEV-1 was tested in LEO, with MEV-2 projected for testing in GEO (Khurelbaatar et al., 2023). Satellites facing the end of their time in service may receive a new lease on life through technologies to extend their capabilities as MEV-1 and MEV-2 operations grow (Redd, 2020). The same MEV technologies can be used to prevent future satellite collisions if enough notification time is granted (Rome et al., 2023).

Most Common Satellite Attacks

Satellite hijacking involves unauthorized access and control over a satellite's systems, which enables an attacker to manipulate the original functions or disturb its operations (Lohani & Joshi, 2020; A. Saad et al., 2019). While satellite hijacking is a substantial concern, it is notable that specific details and techniques vary, while some attacks may be speculative due to their confidential nature. Some examples of typical attacks that could be used to hijack satellites include but are not exclusively limited to (a) jamming, (b) spoofing, (c) physical access/destruction, (d) software attacks, (d) Denial of Service (DoS) attacks, and (e) Man-in-the-middle (MITM; F. Wang et al., 2019; Yue et

al., 2022). Methods used to deter these threats depend on the adversary's or insider threat's capabilities and access. It is crucial for a space agency or organization to identify potential security and reliability risks, thoroughly examine them, and derive valuable insights and defensive measures from the lessons learned.

Satellites communicate through radio waves that send and receive signals from base station antennas on Earth's surface. Since some communications satellites are farther out, they rely on Tracking and Data Relay Satellites (TDRS) to pass on signals. Adversaries could conduct orbital warfare by sending satellites with high-powered microwaves and radiofrequency jammers (Giri et al., 2020). The same technologies to potentially decommission satellites during peaceful operations could be militarized to conduct wartime operations (Giri et al., 2020). The Institute of Electrical and Electronics Engineers (IEEE) has circulated a standard for the letter designation of radar-frequency bands used for radar, satellite, and terrestrial communications (Hakobyan & Yang, 2019). Ground antennas are used for more than just communications; they also function as tracking systems for satellites and space debris. A wide frequency of bandwidths is allocated to satellite communications. Some of the bands include Fifth Generation (5G)-sub-6 Gigahertz (GHz) band (3.3-6.0 GHz), Ku-band (10–16 GHz), and Ka-band (18–31 GHz) (Hassan & Davenport, 2022). When a satellite is in orbit, the orientation of the ground station or terminal antenna plays a significant role in how satellites receive the beam (Hassan & Davenport, 2022). Due to how frequently satellites change orbital plains to dodge space debris, communications antennas, and receivers need to be flexible with rapid reconfigurability capabilities. The traffic in the Earth's orbit is bustling, and

collisions are possible even with the vast amount of space (H. Li et al., 2022; Mrusek & Weiland, 2023). Older satellites are behind the technology curve and rely on older technologies meaning they will remain outdated until they are decommissioned and replaced with updated satellites that benefit from new antennas (Mrusek & Weiland, 2023). According to the (European Space Agency (ESA), n.d.) radars have assigned frequency powers, and various wavelengths:

- High frequency (HF)
  - 100-10 meters (m) wavelength
  - 3-30 megahertz (MHz) of power
- Very high frequency (VHF)
  - 10–1 m wavelength
  - 30-300 MHz of power
- Ultra-low frequency (ULF)
  - 100–30 centimeters (cm)
  - 300-1000 MHz of power
- L Band
  - 30–15 cm wavelength
  - 1-2 gigahertz **(**GHz) of power
- S Band
  - 30–15 cm wavelength
  - 2-4 megahertz GHz of power
- C Band

  - 15-7.5 cm wavelength
  - 4-8 megahertz (MHz) of power
- X Band
  - 7.5-3.75 cm wavelength
  - 8-12 GHz of power
- Ku Band
  - 3.75-2.50 cm wavelength
  - 12-18 GHz of power
- K Band
  - 1.67-1.11 cm wavelength
  - 18-27 GHz of power
- Ka Band
  - 11.1-7.5 Millimeters (mm) wavelength
  - 27-40 GHz of power
- V Band
  - 7.5 mm-4 mm wavelength
  - 40-75 GHz of power
- W Band
  - 4 mm-2.73 mm wavelength
  - 75-110 GHz of power

Most satellite downlinks predominantly utilize the S-band, as it is specifically reserved for Space-to-Earth transmissions (Kobayashi et al., 2019). Ground station sites

like Alaska, Norway, and Chile, which are part of the Near-Earth Network (NEN), are configured to facilitate Space-to-Earth communication links (Kobayashi et al., 2019). The S-band boasts both advantages and disadvantages in terms of technology. Notably, one of its primary advantages is its reduced susceptibility to atmospheric attenuation. This attenuation occurs when a source electromagnetic signal traverses the atmosphere and interacts with gaseous elements, causing its strength to diminish (Saqlain et al., 2021). Conversely, a drawback of the S-band is its requirement for higher pulse power to achieve long-range transmissions (Akasaka et al., 2022). Additionally, satellite operators face the challenge of potential blockages and interference in radar-frequency bands, stemming from mechanical, electronic, and inadvertent jamming issues (X. Zhang et al., 2022).

With S-band being explicitly reserved for Space-to-Earth, comes the danger of being targeted by adversaries wishing to disturb, exploit, or destroy satellite communications (Giri et al., 2020). Countermeasures can be employed and dispersed across various sites to prevent attacks (Y. Zhang et al., 2022). Targeting satellites during control operations, updates, or decommissioning measures could contribute to potential space collisions (Dilworth & Osborne, 2022). A communication satellite that loses communication could steer off its target and collide with another satellite or space debris (Ai et al., 2022).

Table 2

Number of Space Launches Since 2020

Year	Government	Civil payloads	Commercial payloads	Total payloads
2023	0	0	114	114
2022	6	2	1,560	1,568
2021	3	1	1,125	1,129
2020	9	6	848	863

Note. In 2022, there were six commercial payload failures. Non-existing tables were used to pull data for complication from.

Strategies to Deter Cyber Threats

Gaining a comprehensive understanding of the methods employed in satellite communications is crucial for effectively defending them against adversarial attacks. Numerous strategies are dedicated to deterring cyber threats on IT satellite space systems, with the primary objective of bolstering the security and resilience of these systems against potential cyberattacks (Yue et al., 2022). Methods include but are not limited to (a) securing communication protocols, (b) enforcing authentication and access control, (c) conducting vulnerability and penetration testing, (d) continuous security monitoring and incident reporting, (e) software and firmware updates, (f) physical security measures, (g) training and awareness, and (h) redundancy and built-in resilience (Falco, 2020; Manesh et al., 2019; Manulis et al., 2021; Rome et al., 2023).

Strategies to Protect Satellite Support Controls and Facilities

Ensuring the protection of physical buildings that house critical infrastructure components for space operations is equally vital as safeguarding the space assets themselves. Physical security constitutes an essential element of a comprehensive security strategy, working in conjunction with space system protections to establish comprehensive security measures (B. Chen et al., 2020). The Satellite Control Network (SCN) is a widespread system constructed to monitor and manage satellites and serves as a vital component of the military's space operations, enabling them to maintain control, communication, and coordination with their satellites (Ji et al., 2021). The SCN incorporates an infrastructure of ground-based control stations tactically located around the globe. Adversaries wishing to hack satellites can do so through various means and platforms such as Industrial Control Systems (ICS), processing centers, end-user systems, or satellite communication devices. Comparable to the SCN is the SSN as it is also a comprehensive system managed by the U.S. military and other organizations to monitor and track space assets and debris, ultimately playing a vital role in safeguarding the safety, security, and sustainability of space operations. (Kawamoto et al., 2020).

A hacked satellite can be made inoperable, becoming space debris, and ultimately contributing to the potential Kessler Syndrome phenomenon (Barato, 2022). Technologies exist to destroy satellites that are currently in orbit (Zhao et al., 2022). Destroying satellites in orbit will only create more space debris and add to the Kessler Syndrome phenomenon predictions. Close-call collisions are becoming more common due to space debris and satellites in orbit (Halawa et al., 2020). With the raised number of

close collisions comes the need for expanded monitoring and reaction procedures for worst-case scenarios (Xie et al., 2020).

Various attack vectors and adversaries could be behind attacking satellites under the control of the government, military, or commercial owners. Advanced Persistent Threats (APT) can be carried out by nation-state actors, nonstate actors, or lone wolves (LaMar et al., 2022). Common Vulnerability Exploits (CVE) is an avenue that various attackers could use to gain unauthorized access to satellite systems, control systems, monitoring systems, transportation systems, or the ICS used to monitor the storage of satellites (Nguyen & Sparks, 2020). Satellites and their systems have been compromised in the past, and some systems could have DoS attacks lying dormant and awaiting activation. Predicting satellite attacks can be tricky unless intelligence is gathered that forecasts or alerts victims of an incoming attack (Raguraman et al., 2020).

Transition and Summary

In section 1, I provided the background to the problem, the problem and purpose statement, the nature of the study, the research question, and the interview questions. My conceptual framework was introduced, and literature was provided to merge the ideas of several researchers. Satellite technologies are ever evolving, and various methods are being proposed to decommission them from orbit once their purpose is served. The lifespan of a communications satellite can be cut short by collisions, kinetic attacks, and cyberattacks. A result of rouge pieces of debris from satellites and spacecraft could set off a chain reaction known as the Kessler syndrome if they were to start colliding. Uncontrolled collisions could impact billions of individuals on Earth who rely on satellite

communications for daily operations and functions. The conceptual framework establishes a notion that space agencies and space professionals across the globe may have the internal expertise to rapidly decommission satellites from LEO without contributing to Kessler syndrome. The benefit of rapidly decommissioning satellites from LEO will have a significant impact on social change because the human race has become accustomed to daily functions enabled by IT satellite communications. These functions and services include ATM use, GPS, telecommunications, and weather forecasting. Furthermore, the literature review considered the causes of satellite collisions caused by space debris or targeted cyberattacks. Also, the literature review mentioned proposed and tested strategies to decommission IT satellites in a safe way.

In Section 2, I will restate the problem statement and discuss the role of the researcher with respect to this qualitative pragmatic inquiry. Also, I will talk about the research methods and design in greater depth in order to support and justify my selection. Section 2 will highlight my strategy for the data collection and analysis and explain the method of how I will ensure reliability and validity within this specific study.

In Section 3, I will accomplish the functions mentioned in Section 2, specifically performing semi-structured interviews, gathering data, and then transcribing the data for analysis. While collecting data for analysis, a primary focus will be placed on the procedures outlined to ensure validity and reliability are at acceptable levels and biases are reduced to a minimum. Finally, I will present an analysis of the data collected with a trusted and reliable application used by other professionals.

Section 2: The Project

In Section 2, I restate the purpose of the study and detail my overall role as the researcher. I also discuss the research method and design, selected population, and sample size. The selected protocol for interviews and how data were collected for analysis are described. Section 2 also includes a discussion of the reliability and validity of the study.

Purpose Statement

The purpose of this qualitative pragmatic inquiry study was to explore strategies used by IT satellite managers in the space industry to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. The participants were current and prior space agency contractors working for large government institutions with experience in satellite operations and construction. The geographical location of the study was the surrounding areas of Cape Canaveral, Florida. The implications for positive social change include the shift in focus for space agencies across the globe to (a) potentially clean space debris before crashing debris hurts those on Earth, (b) link several nations together with the goal of not generating space debris, and (c) use new technologies to prevent satellites from becoming weaponized.

Role of the Researcher

In this study, I was the researcher, and in this subsection, I share my experience as a subject matter expert and highlight the topics under discussion. In qualitative research, the researcher collects data to recognize cause and effect and identify trends (Bhangu et al., 2023). From the year 2007 to the present, I have been involved in basic IT operations

as they evolve into defensive cyber operations and play a part in the shift from supporting space launch assets to defending space launch assets. Between the years 2019 to 2023, I primarily focused on managing teams and toolsets dedicated to protecting satellite control systems, payload storage units, and launch support systems. During that period, I had to monitor, detect, and report suspicious exploitations while conducting penetration testing to harden systems to deter vulnerabilities concurrently. My support for these satellite control systems, payload storage units, and launch support systems was successful. Because of my direct relationship with protecting satellite control systems, payload storage units, and launch support systems and being a part of the satellite protection community, my role as the researcher could be potentially viewed as biased. Due to my oversight of operations, I could have potentially swayed the interviews to reflect my personal views and experience concerning the phenomenon. Nevertheless, biased opinions and perceptions of biased views were alleviated by deploying transparency and deliberate interrogations of sources utilized within the study in accordance with (IAW) suggestions from (Gerson & Damaske, 2020).

For this pragmatic qualitative inquiry, I gathered data from space agency professionals primarily involved in satellite design, cyber protection, and satellite de-orbiting. Before collecting data and interviewing the participants, I completed the Doctoral Student Researchers course provided by the Collaborative Institutional Training Initiative (CITI). The CITI training covers the historical development of human subject protections, ethical issues associated with human subject research, and current regulatory and guidance information. The CITI training course ensures researchers uphold guidance

and best practices for interviewing humans. The CITI training course ensures the protection of human subjects through (a) defining ethical boundaries, (b) defining principles structured by *the Belmont Report*, (c) discovering potential risks in research, (d) protecting vulnerable populations, (e) gaining informed consent, (f) ensuring privacy and confidentially, and (g) ensuring adherence to Health and Human Services (HHS) 45 Code of Federal Regulation Part 46 that requires substantive and procedural requirements for interviews and institutions (Office for Human Research Protections, 2021).

All interviews occurred after I was granted Walden University Institutional Review Board (IRB) approval. The interviewees and participants were treated respectfully, and their identities were masked. The interviewees and participants within the study were autonomous and made aware of any associated risks within participating in the study before they took part in it. To remain in accordance with Health and Human Services 45 Code of Federal Regulation Part 26 and *the Belmont Report*, all interviewees and participants should be treated equally, and no compensation or payments should be offered to volunteers (Husband, 2020). I only selected and interviewed individuals that were not vulnerable to manipulation or exploitation. These comprised of but were not solely limited to children and mentally or physically ill individuals. The selection of the subjects required in-depth evaluation and consideration to ensure none of the participants fell into a category of potential exploitation, which aided them in keeping clear of risks (see Pritchard, 2021).

Researchers conducting qualitative studies with semi-structured interviews must have rationale for an interview through the deployment of protocols (Myers & Newman,

2007). Maintaining order and structure are crucial to collecting information from the volunteer interviewees (Dorji & Tenzin, 2021). Having protocols in place ensures that the participant's time will not be wasted and will keep the interview on track. Protocols can be summarized as a guide for the interviewers to formulate and plan the required questions (Doody & Noonan, 2013). I developed an interview protocol (see Appendix B) that contains instructions and guidance that I strictly adhered to while conducting interviews. I asked the planned questions at the beginning of the interview and followed the protocol to the end of each participant's interview. Each interviewee was asked the same interview questions in the same order to ensure data were collected in order. I framed the questions and placed them in a specific order to gauge the participants' experiences in detail. Protocols were also put in place to conclude the interviews.

Measures must be in place to ensure that removing a layer of bias does not increase another bias level; moreover, the tools employed by the researcher can introduce or decrease bias as well (Z. Chen et al., 2023). The best practice for a researcher to mitigate the impression of bias is to be transparent about their roles, past experiences, and background as it relates to the study. To mitigate bias, I applied a conceptual framework (i.e., the ISTISM) to this study to diminish bias.

Before beginning a study, it is crucial to have a plan to extract critical data and minimize the presence of bias (T. Li et al., 2019). T. Li et al. (2019) suggested (a) for the researcher to collect data separately for each intervention group of interest, (b) to understand and familiarize themselves with relevant elements of the study, (c) to facilitate the risk of bias assessment, and (d) to enter the collected data into software that

allows for estimations and calculations. In my role as the researcher, I adhered to these suggestions and reached out to my committee throughout the study for their guidance.

Participants

I based the selection of participants on the core research question. The research questions should be the top consideration when choosing individuals to interview and participate in a qualitative study (Morgan, 2022). The selected participants had extensive knowledge regarding space industry strategies, defensive cyber operations, and satellite communications. Some participants were contractors and civilian employees working within space launch organizations, including the government and commercial platforms. Foreign governments were not contacted for interviewing or information. I did not interview active-duty military members or anyone assigned to clandestine operations to prevent potential data leaks. The selected participants had at least 5 years in government or commercial support of space industry strategies, defensive cyber operations, and satellite communications.

Selected participants and interviewees had to have directly experienced a situation or exercised scenarios related to the research question. I collected the experiences of the participants as data to analyze the strategies they used as corrective actions. The data were also used to uncover trends in where improvements can be made based on collective suggestions from the interviewees. Those who have dealt with the phenomenon firsthand will have valuable information to share during interviews (Bearman, 2019).

Due to my role in the U.S. Space Force and the IT community within various government and commercial organizations, I have developed professional relationships

with potential interviewees and participants due to how closely we reside. In my current role, I directly support launch operations on the eastern coast of Florida and contribute to defensive cyber operations through penetration testing. This type of role and support to commercial and government agencies have allowed me to build rapport with potential interviewees and participants. A professional relationship with potential interviewees and participants can allow for in-depth conversations and the interviewer to access needed information (DeJonckheere & Vaughn, 2019). A researcher's personal knowledge of the research subject can directly relate to rapport building (Mirick & Wladkowski, 2019). I used professional social media platforms, such as LinkedIn, to recruit and connect with participants outside of local networking of space professionals.

Research Method and Design

Method

The aim of this study was to identify strategies used by IT satellite managers in the space industry to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. There were a small number of organizations to choose from for the recruitment of participants because of my physical location, but even so, I wanted to comprehend the depth of the strategies of space agencies. The qualitative method was most suitable to achieve this goal. Qualitative data can be saturated through triangulation from multiple sources of data (Fusch et al., 2018).

I considered quantitative, qualitative, and mixed-method approaches for the current study. The research question plays a role in the selection of a research study design that will genuinely answer the question (Fusch et al., 2018). Quantitative research

is employed by researchers to generalize a sample across a wide population with an effort made to compare a sample to an experienced counterpart (Zyphur & Pierides, 2017). I conducted this study to explore strategies to rapidly decommission IT satellites without contributing to Kessler syndrome without the intention of gathering statistical data for generalization; therefore, I did use the quantitative method.

The mixed method is a combination and overlapping of both qualitative and quantitative approaches to generate a unique perspective of the research problem (Plano Clark, 2017). The varying methods can produce different answers during a study (Bergen & Labonté, 2020). There can be a time and place to use the mixed-method approach to add value to the overall study; however, the mixed-method approach did not align with my intentions in the current study. Selecting a mixed-method approach for a study requires integrating quantitative and qualitative sources backed by a rational foundation (Tashakkori et al., 2020). The main reasoning behind selecting the qualitative method over the quantitative approach is to pilot toward the "why" and "how" of the research problem that cannot be observed in a quantitative study (Lo et al., 2020).

Space professionals should consider the protection of space as space proliferation grows at an extreme rate (Adushkin et al., 2020). Governments and commercial and private space agencies should have ethical standards, practices, and strategies to protect their domain of profession. Through use of the qualitative method, I, as the researcher, collaborated with the participants to isolate objective information that correlates with the research question. Although the quantitative approach could have been used, the need for a deeper dive into the participants' experiences was needed, and the current study did not

depend on probability and random samples to answer the research question; therefore, the qualitative method was selected.

Research Design

I considered the following qualitative research designs: the narrative design, ethnography, a single case study, and pragmatic inquiry. I chose not to select a narrative design for this study because this design requires gathering in-depth, firsthand stories as raw data, including individuals' experiences, to illustrate a life experience and discuss the meaning (see Butina, 2015). Although I could have benefited from raw data through a narrative design, the information gathered could be seen as subjective, and it may have been challenging to gather enough stories. The narrative design has been used in various disciplines with the intention of learning more about culture, historical experiences, identity, and lifestyles; however, the narrative design is sometimes criticized because it is story based and may divert from the true intention of diving deep into the phenomenon (Butina, 2015). In the current study, I focused on historical events that took place and were not from the interviewee's perspective. Due to these reasons, I did not use a narrative design because it was not suitable.

I chose not to select an ethnographic design for this study. The ethnographic design grants the researcher direct access to the culture and practices of a group (Wutich & Brewis, 2019). Ethnography links the researcher with the identity of the interviewee's race, age, and gender (Krause, 2021). In the current study, race, age and gender did not play a role because the study heavily relied on the participants' experiences in the field. Ethnography encompasses subjective interpretation and can be problematic in

maintaining the necessary distance required to analyze a group of interviewees (Knott et al., 2022). The ethnographic design allows for the use of informal interviews and observations where the interviewer is embedded with the participants (Sorce, 2019). I preferred to deploy semi-structured interviews, avoiding the need to observe interviewees who had experienced the past phenomenon. The ethnographic design may take extensive time because the aim may be to modify existing theories or develop an entirely new theory (Caskurlu et al., 2021). My goal was not to develop a new theory or modify an existing one; therefore, an ethnographic design was unsuitable for the current study.

I did not to select a single case study design. The single case study design may provide a practical alternative to large group studies by randomized clinical trials to collect repeated measures for manipulation of an independent variable (Lobo et al., 2017). Single case study measurements can be difficult to replicate and may require extensive amounts of time (Flyvbjerg, 2006). Single case studies can be resource-intensive and time-consuming and are limited in their ability to generalize findings to broader populations or contexts. The current study aimed to draw conclusions that could be applied more broadly, making a different research approach more appropriate. Although single case studies produce high internal validity and address a phenomenon, it was deemed unsuitable for the current study as I wished to have a broader approach.

I employed a pragmatic inquiry design for this study. Pragmatic inquiries emphasize that knowledge is based on experiences, and the design heightens the researcher's ability to analyze organizational or industry practices through experience as well as action (Kelly & Cordeiro, 2020). The pragmatic inquiry design allows for an in-

depth understanding and future analysis (Darke et al., 1998). My study can be used in the future for further analysis and expansion of identifying strategies. A pragmatic inquiry places weight on (a) actionable knowledge, (b) identification of the interconnectedness linking experiences, and (c) a view of inquiry as an experiential process (Kelly & Cordeiro, 2020). The pragmatic inquiry research method incorporates operational decisions based on best practices to find answers to the research question(s) developed by the researcher (Metcalfe, 2008). The use of the pragmatic inquiry design assists researchers with conducting a study in innovative and dynamic approaches to answer the research question(s) (R. Johnson & Onwuegbuzie, 2004).

I achieved data triangulation method using numerous sources to achieve full saturation and address the research question. Carter et al. (2014), Jick (1979), and Patton (1999) defined triangulation as the use of multiple techniques or data sources in qualitative research to foster a comprehensive understanding of a phenomenon. Triangulation can reduce bias and amplify the saturation of collected data through using participant's responses and examining what can be observed (J. Johnson et al., 2020). I used document reviews, surveys, interviews, and observations to achieve successful triangulation and saturation. Standardization is crucial and needed to gather the most appropriate data; all interviewees must be asked the same questions to decrease bias from interviewer influence and increase data saturation (Mwita, 2022; Ranney et al., 2015). The interviews and documents collected were unclassified.

Population and Sampling

This study will target participants who are current or prior contractors working for space agencies with experience in satellite operations and manufacturing as well as potential cyberattacks. The participants will have some form of satellite operations and manufacturing experience along with an understanding of cyber protection requirements. Additionally, the participants had advanced cyber security awareness training which is the basis for effective IT hygiene and threat aversion. In order to gather rich information and outside of the box thinking, two launch bases, two manufacturing sites, and one headquarters with direct support to launch operations, satellite creation, and defense will be targeted. The eligible and available participants of these sites will be interviewed until thematic saturation is met, and no new trends emerge. For a qualitative study, thematic saturation is achieved when no new themes materialize from the participant's interview responses throughout the study (Braun & Clarke, 2021).

Criteria for selecting participants will include (a) alignment with research question, (b) diversity, (c) inclusion/exclusion, (d) availability and accessibility, (e) informed consent, (f) saturation, (g) cooperation and engagement, (h) researcher bias and (i) practical constraints. I will only select participants based on their relevance to the research question and my topic of study. The participants with the most relevance will possess the necessary knowledge or experience to provide valuable insights into the phenomenon under study (Alhazmi & Kaufmann, 2022). I will select participants from diverse backgrounds in order to gather varying viewpoints. Diversity in semi-structured interviews can result in the researcher gathering significant amounts of data to compile

for theme analysis (McIntosh & Morse, 2015). Diversity can capture a wide range of perspectives and experiences related to the research topic and consists of knowing age, gender, ethnicity, and socioeconomic status (Budhu et al., 2021). Inclusion and exclusion criteria will be set to define the characteristics or attributes that make an individual eligible or ineligible to participate in the study. For example, active-duty military members will not be interviewed although they may be space professionals who fit the criteria elsewhere. The practicality of recruiting and accessing potential participants will be considered in the availability and accessibility steps because those selected must be willing to commit to the study requirements. Finding willing and participative interviewees is essential to propelling a research study forward (Oliffe et al., 2021). The informed consent of all participants will be obtained prior to carrying out interviews or using their responses in data analysis. All participants will be fully informed about the study's purpose, procedures, and potential risks before they participate.

Saturation will be apparent in my study, to ensure that the data collected is thorough enough to tackle the research questions. For qualitative studies, starting with a sample size of 12 is advisable, while also considering the research question and the quality of the selected samples (Hennink et al., 2016). There is no fixed, set, or universally proposed sample size in qualitative studies when compared to quantitative studies because quantitative studies rely on statistical power calculations to determine the needed sample size. In qualitative research, the sample size is typically influenced by the concept of achieving data saturation. The actual number of participants or interviews required to attain data saturation may vary depending on the complexity of a research

question, the depth of the data collected, and the overall diversity of perspectives encountered. Data saturation is the point in the researcher's process where the newly gathered data no longer leads to new or meaningful insights. At the point of data saturation, the researcher should see that enough information has been collected to adequately explore and understand the research question, topic, and phenomenon. Since my study is qualitative, I will aim to achieve data saturation rather than having a predetermined sample size. I will start with a smaller sample size of six and analyze the data as it is collected. I will continue data collection through purposeful sampling until I reach a point where new data does not yield additional insights or themes. If new insights or themes become apparent, I will expand the interviews until data saturation is achieved by no longer uncovering new insights or themes.

Purposeful sampling and snowball sampling are two distinct methods applied in qualitative research in order to select participants (Mweshi & Sakyi, 2020). Purposeful sampling is a non-random sampling method where a researcher intentionally selects participant(s) based on specific criteria which align with the research objectives. Snowball sampling is a non-probabilistic sampling technique frequently utilized when investigating rare or hard-to-reach populations, where potential participants are scarce or unknown initially. My study will use purposeful sampling in order to select participants who possess relevant knowledge, experiences, or characteristics needed for addressing my research questions properly. Although purposeful sampling will allow for the targeting of specific groups or individuals with valuable insights, it may not provide a representative sample of the larger population. With purposeful sampling, there is a risk

of a researcher introducing bias in the selection process, because the researchers' judgment plays an ample role in participant recruitment.

Snowball sampling will not be utilized because the process of finding participants through referrals can be time-consuming, and there is a risk of missing out on certain segments of the population. Just like purposeful sampling, there is a potential for bias because snowball sampling also may not be representative of the entire population, as participants are recruited through personal networks, leading to potential bias in the sample. Purposeful sampling will gather the number of participants needed and snowball sampling is not required because there is not a suspected hidden population. Snowball sampling also does not hit my study because members suggested that interviews may be outside of my targeted group.

Semi-structured interviews rely on the researcher asking key questions in order to open discussions around identified themes or uncover new themes (Mak & Singleton, 2017). I will select the most qualified satellite operators, satellite manufacturers, and space professionals who protect or defend satellites. I will ask the participants the same questions in semi-structured interviews and triangulate three data sources by (a) relating the descriptions given by the participants about the phenomenon, (b) reviewing and investigating industry documents, (c) and performing member checks. Member checks involve seeking feedback from participants to ensure the accuracy of the study (Motulsky, 2021). I will carry out the interviews utilizing three methods (a) in person with notes to capture verbiage, (b) through Video Teleconferencing (VTC) applications and/or platforms such as Zoom and Skype with notes to capture verbiage, and (c) email

responses from space professionals that can be directly uploaded into the qualitative analysis software. Email interviewing refers to running an interview via e-mail, which allows the participant to provide responses at their own pace and over an extended period of time if they are unable to participate in traditional interviewing methods. Email interviewing will be the last resort if the selected participant is unable to communicate in person or via VTC methods. In addition to in-person and VTC methods, the interview sessions will be recorded to ensure I as the researcher can listen to the verbiage again to prevent the loss of any crucial information. Recording interviews with the participant's consent can significantly assist researchers in systematically categorizing information and data, thereby enabling the identification of prominent themes that emerge from the semi-structured interviews (D. Wang et al., 2022).

Ethical Research

My study will take ethical considerations into account. As the researcher, I will protect the participants' confidentiality, privacy, and well-being during the study. In research, the researcher must take ethical principles into account to ensure participants are protected (Sim & Waterfield, 2019). In my study, I will select participants who showcase a willingness to engage actively and openly to share their experiences and perspectives. Shared in-depth experiences and perspectives from active interviewees can assist the researcher gather a large amount of data to enrich their study (Winwood, 2019). I will strive for neutrality and impartiality in the selection process to ensure I am not inputting bias into the study. A practical constraint of timelines will be considered for my qualitative study while selecting participants.

The Belmont Report lists key aspects needed to ensure ethical considerations are employed by researchers. Three primary areas of consideration within *the Belmont Report* include (a) respecting individuals, (b) beneficence, and (c) justice (Office for Human Research Protections, 2021). In this study, participants will be respected by protecting all participants, professionally speaking to them, and ensuring that they do not feel overwhelmed by questions. Beneficence will go hand in hand with respect as all participants will be treated kindly and not placed in uncomfortable situations. Justice will be reflected by properly adhering to guidelines and treating all participants equally no matter their background. Furthermore, I completed the CITI training course which teaches researchers the knowledge required to uphold guidance and best practices for interviewing humans. All interviews will occur after IRB approval is granted. Throughout this study, I will adhere to CITI training, *the Belmont Report*, and IRB guidelines. *The Belmont Report* has two distinct outcome objectives which include the contribution of knowledge and the improvement and well-being of participants/interviewees (Friesen et al., 2017). Before the IRB, I will assess the associated risks and mitigation methods required to participate in this study. No risks will be introduced that are beyond their current function within their occupation or operational contracts. Beneficence is being considered because the resulting yield from this study will help participants improve strategies to properly decommission and protect IT satellites in LEO that are vulnerable to cyber-attacks.

Participants will have the liberty and ability to withdraw from the study anytime they wish to by generating an email outlining their intention. Furthermore, during the

interview process, I will make it clear that they can withdraw from the study at any time or not answer a question if they feel like it could become classified material. If a participant wishes to withdraw from the interview, I will terminate the discussion, delete notes taken, and erase any recordings. The protection of participants is crucial due to the rise in privacy leaks which can be deterred by protecting research participants (Wiles et al., 2008). To ensure privacy and the potential for reprisal, no names of individual organizations or individuals themselves will be used in the study. The names of the participants will be removed from notes and journals and assigned a number as an alias. Participants in a study must be optional with a preference towards autonomy (Johansson et al., 2017). I will not provide any compensation for individuals taking part in the study, and no additional expenditure will be incurred throughout the study. It is not a recommended practice in qualitative studies for a researcher to encourage payment however reimbursement of expenses can be ethical (Millum & Garnett, 2019).

To align with the goals of *the Belmont Report*, I will ensure that all participants are granted full access to the study results for possible inclusion in their strategies to decommission and protect IT satellites in LEO that are vulnerable to cyberattacks. Additionally, to amplify respect for the participants, I will provide each volunteer interviewee with a consent form describing the purpose of the study, associated risks, details of anonymity, and the projected benefits. A copy of the informed consent form will be attached in Appendix C. All gathered data will be protected through encryption and strong password safeguards for 5 years in a locked safe in order to align with the

policy set by Walden University. My IRB approval number for this particular study was approval number 11-22-23-1014975 and I received it on 22 November 2023.

Data Collection

Instruments

Collected data for a study introduces challenges for the researcher along with the interviewees. Some challenges which may arise include but are not limited to building rapport, lack of experience with interviewing by the researcher and a participant's unwillingness to partake in a study (Azad et al., 2021). The main instrument I will use is the relationship between the participants to collect data from interviews for further analysis. Semi-structed interviews allow for very open-ended questions and discussions which bring forward detailed explanations of the topic(s) (Husband, 2020). In qualitative studies, the researcher assumes the vital role of the primary data collection instrument, establishing meaningful relationships with the participants, skillfully conducting interviews, and expertly analyzing the gathered data (Sürücü & Maslakci, 2020). The consistent and meticulous application of the instrument to all participants within the same context significantly enhances the study's validity (Oldland et al., 2020). By employing semi-structured interviews with all participants, I aim to pose open-ended questions that will effectively prompt and encourage detailed explanations of the phenomenon at hand. Semi-structured interviews serve as a valuable tool for researchers to acquire deep insights into the phenomenon, by allowing for the capture of a unique perspective of the participant (Ruslin et al., 2022). Furthermore, open-ended questions can result in follow up questions to guide conversations about the interview/research questions. The interview

protocol which is outlined in Appendix B will be used by myself as the researcher to ask questions to the participants in a uniform manner. Before the interviews are conducted, I will test out my interview protocol with peers and the chair to confirm it is clear and concise without questionable verbiage. Conducting a preliminary trial of the interview protocol before commencing the actual study interviews can enhance the interviewer's comfort level, leading to a higher quality of gathered information for subsequent data analysis (D. Johnson et al., 2021). Upon completion of the transcription process, I will diligently conduct member checks with the participants, aiming to validate all the gathered information. This critical step will afford participants the opportunity to review and make any necessary changes to ensure an accurate representation of their input. Member checking represents an invaluable approach to both validating and enriching the quality of the data gathered in the study (Coleman, 2022). The application of members checking in this study will benefit the overall study and strengthen its validity.

Data Collection Technique

For my planned research, I will be the primary tool for collecting data and conducting semi-structured interviews and observation of participants. Each interviewee will be meticulously guided through the interview protocol as outlined in Appendix B, thereby ensuring comprehensive coverage of all pertinent areas in a systematic and thorough manner. Interview protocols play a pivotal role in guaranteeing that each session is conducted within a designated timeframe, effectively addressing the research question, minimizing bias, and bolstering the overall validity of the study (Stone et al., 2023). The data collected will include responses to targeted interview questions that

provide insight into the strategies that are used to properly decommission satellites rapidly out of LEO if targeted by cyberattacks. Second, I will collect internal organizational documents such as doctrine and publicly released strategies and innovations to de-orbit satellites. The interviews and documents collected will be unclassified. Databases used to pull information consist of Ulrich's Web Global Serial Directory, Google Scholar, and the Walden University Library. Upon the completion of interviews and transcriptions, I will perform member checking to thoroughly validate and authenticate the outcomes of the study. Semi-structured interviews and observation of participants in qualitative data collection techniques offer a range of advantages and disadvantages, with each being suited to special research goals and contexts (Stone et al., 2023). A major advantage of semi-structured interviews is that they allow researchers to probe deeply into participants' experiences, perceptions, and overall emotions (Mahat-Shamir et al., 2021). Utilizing semi-structured interviews may generate rich and detailed data that can provide a deep understanding of a complex phenomenon. A disadvantage of semi-structured interviews and observation of participants is that they involve the researcher's interpretation and analysis, which may introduce subjectivity (Magaldi & Berler, 2020). Researchers' biases and preconceived notions can influence the data and affect the overall interpretation. Finally, semi-structured interviews and observation of participants in qualitative data collection can be quite labor-intensive, due to the time needed for transcribing, coding, and analyzing data (Lester et al., 2020).

Data Organization Techniques

Maintaining data in an organized manner is of utmost importance, as it enables its effective reuse, and seamless retrieval, and facilitates study reproduction for future analyses and investigations (Ningi, 2022). In this study, I will employ Microsoft Excel software to document emerging themes. In qualitative studies, Microsoft Excel can be used to document and organize data while leveraging its powerful features which enables researchers to readily identify, filter, and interpret relationships between figures (Pathiranage et al., 2020). Understanding the relationships and emerging themes enables the researcher to gain a deeper understanding of the data at hand.

Throughout the study, the participants will be assigned numerical aliases, and a redaction of their location and true names will be carried out to ensure complete anonymity. The data collected from each participant will serve as a valuable resource in cataloging and unveiling emerging trends that manifest during the course of the interviews. While conducting a research study, it is imperative to catalog raw data in a manner that facilitates effective filtering, thereby supporting the selection of pertinent data that directly addresses the research question (Boddy et al., 2017). Along with Microsoft Excel being used to sort data into categories, I will also take physical notes that can be transcribed into Microsoft Excel if I am unable to use a laptop to type notes. Every note that I record will be carefully dated and accompanied by a thorough narrative, detailing the factors that prompted that particular thought and its subsequent impact on the study. Journals can serve as a tool to recognize underlying themes while reminding researchers of potential biases and confidentiality concerns while being adaptable in

various formats (Church et al., 2019). All raw data collected during the interviews will be password-protected and encrypted on a primary and backup hard drive. The primary and backup hard drives will be labeled with a destruction date and placed in a safe for five years. Once the destruction date arrives, the data will be permanently deleted from the primary and backup hard drives.

Data Analysis Technique

A modified van Kaam method will be utilized to identify themes from qualitative data gathered to compare and contrast accounts of those who experienced the phenomenon. The modified van Kaam method approach is a qualitative research technique used to analyze textual data, such as interviews, focus group transcripts, or written documents (Anderson & Eppard, 1998). Furthermore, NVIVO qualitative analysis software was employed to conduct thematic analysis through a combination of inductive and deductive analysis approaches to derive codes and themes. NVIVO software supports researchers in organizing and analyzing intricate word-based and multimedia data. The software allows researchers to classify, sort, and arrange large amounts of information quickly while accommodating a wide range of research methods (X. Feng & Behar-Horenstein, 2019). The interviews in my study will be transcribed through the use of specialized software called Express Scribe along with a quality assurance check for any mistakes. Express Scribe is a specialized audio player software designed for PC or Mac, with the primary purpose of aiding in the transcription of audio recordings by professionals. Selecting proper transcribing software is essential because an inaccurate transcription of an interview can render a study invalid (J. Johnson et al.,

2020). Using software to transcribe the interviews prevents potential issues with the confidentiality of hiring a human third party.

I will read the transcribed interviews in order to identify various viewpoints which may point to different themes. Once new themes are discovered, each theme will be assigned a specific code. After assigning codes to these themes, they can be systematically filtered to extract information that directly addresses the research question posed during the interview. By employing the modified van Kaam method in a qualitative study, researchers can derive meaningful codes that reveal overarching themes and sub-themes based on the gathered responses (Phillips-Pula et al., 2011).

To achieve comprehensive saturation and arrive at the most robust findings for the research question, a researcher can employ the triangulation method, drawing on a diverse array of sources (Carter et al., 2014; Jick, 1979; Patton, 1999). For this study, I will use data triangulation to foster a comprehensive understanding of a phenomenon. Triangulation can efficiently mitigate bias and amplify data saturation by incorporating participant responses and observations, resulting in a comprehensive and strong analysis. (J. Johnson et al., 2020). I will use document reviews, surveys, interviews, and observations in order to achieve successful triangulation and saturation. Standardization plays a crucial role in gathering the most pertinent data; to minimize bias resulting from interviewer influence and maximize data saturation, all interviewees will be asked the same set of questions (Ranney et al., 2015). Asking the interviewees, the same questions will allow for the researcher to discover trends and recurring observations that can be used in coding and analysis (Bearman, 2019).

Reliability and Validity

Reliability

The reliability of the study relies on the reliability of the instruments, interviews, and survey questions used by the researcher (Khoa et al., 2023). Utilizing the same instrument across various participants to generate the same results creates consistency in the study (Hemmler et al., 2022). It is crucial for scholarly researchers to follow thorough processes in order to achieve validity within the study. Qualitative studies do not rely on statistical data like quantitative studies which may cause qualitative studies to be prone to subjectivity (Mwita, 20222). In this study, I will enforce qualitative standards from the beginning to prevent the study from becoming void due to failure to follow validity processes. Moreover, the validity depends on constructs used throughout the study and is obtainable through the employment of semi-structured interviews (Ruslin et al., 2022). Demonstrating credibility as a researcher requires insurance that the information collected is accurate and properly represents the participants' perspectives and experiences. A researcher can achieve this through persistent engagement with the participants, applying triangulation methods on data from multiple sources, and applying member checking, to have participants review and validate the findings (Motulsky, 2021). As the researcher, I will ensure dependability by maintaining an organized and transparent process during the study. Researchers should always document their decision-making processes, methodologies, and any changes made throughout the study (Shaker et al., 2021).

Validity

In a qualitative study, internal validity and external validity are two essential traits that refer to the accuracy and generalizability of the research findings (Oldland et al., 2020). Internal validity highlights confidence in the study's ability to draw accurate conclusions about the relationships observed among the participants, and triangulated focused on phenomena under investigation (Daubner et al., 2023).

Dependability

As the researcher I aim to achieve persistent engagement with the participants, apply triangulation methods on data from multiple sources, and deploy member checking. The use of member checking involves having the participants review and validate the findings (Motulsky, 2021). Member checking allows the participants an opportunity to clarify any misunderstandings or misinterpretations that may have arisen during data analysis (Megheirkouni & Moir, 2023). Moreover, member checking may increase the strength of themes through the refinement and adjustment of emerging themes or patterns in the data through collaboration with the participants (Coleman, 2022).

Transferability

In order to amplify transferability, this study will contain a detailed description of the study context, participants (with names and actual positions redacted), and data collection procedures used, which will allow other researchers to calculate the applicability of the findings to diverse contexts and or settings. External validity highlights the degree to which the study's findings can be generalized outside the specific sample or population and the use of the context in the research (Taherdoost, 2022). This

study's findings may have the potential applicability of future qualitative studies when applied to similar situations or settings.

Credibility

As part of the study and methods to increase validity, I will seek feedback from colleagues and experts in the field to ensure reliability and legitimacy. Credibility is a key criterion for assessing the quality and rigor of qualitative research (N. Singh et al., 2021). Credibility is closely tied to internal validity in qualitative research because it focuses on the researcher's ability to ensure consistent, accurate, and truthful representation of the interviewee's perspectives, and experiences (Stahl & King, 2020). To enhance my study's credibility, I will use data triangulation, member checking, peer debriefing, negative case analysis, and peer reviews. Negative case analysis will only be applied if an instance comes to light which does not fit within emerging patterns or themes.

Confirmability

Confirmability refers to the degree to which the research findings are grounded in the collected data and interpretations rather than being influenced by the researcher's bias, values, or personal preconceptions (Carcary, 2020). As the researcher, I will ensure that the findings are grounded in the factual data and not influenced by the researcher's preconceptions or biases. To strengthen confirmability in my study, I will employ several strategies which include, explain researcher bias awareness, using peer reviews, employing negative case analysis, member checking and showcases the logical flow of raw data to final interpretation analysis through clear data trails. A researcher paying close attention to confirmability, aids in the diminishment of their personal biases and

subjectivity on the research outcomes (Bush & Amechi, 2019). This increases the study's confirmability and validity and ensures conclusions drawn from the study are securely rooted in the thoroughly collected and analyzed data, which will extend the overall authenticity and dependability.

Data Saturation

Triangulation serves as a method to mitigate bias and enhance data saturation by integrating participant responses and observational insights (J. Johnson et al., 2020). Employing a combination of document reviews, surveys, interviews, and observations, I aim to ensure a robust triangulation process that enhances data reliability. A pivotal aspect involves standardization, necessitating uniform questioning for all interviewees to mitigate interviewer influence and bolster data saturation (Ranney et al., 2015). This approach underscores the commitment to obtaining the most accurate and comprehensive data possible.

Transition and Summary

In Section 2 of the study, the purpose statement was revisited, and a comprehensive exploration of the researcher's role and scholarly processes was discussed. Shifting focus to Section 3, I will present an overarching view of the study, thoroughly showcase my findings and results, and engage in reflective discussions regarding their implications for professional practice. Furthermore, I will present actionable recommendations as part of section three. As the section draws to a close, I will offer valuable insights for future research pursuits, provide personal reflections on the study, and provide a conclusion. In Section 3, I will provide an overview of the study, present

my findings, discuss the applications to professional practice, and state recommendations for potential action. At the end of this study, I will provide recommendations for further research, thoughts, and my final conclusion.

Section 3: Application to Professional Practice and Implications for Change

In this section, I present the outcomes of the qualitative study and explore the connections between the identified themes and their relevance to professional practice. To arrive at the findings, I conducted a comparative analysis utilizing the ISTISM as the conceptual framework. In Section 3, I also discuss the implications of the results for social change and provide actionable and realistic recommendations. Concluding the study, I offer suggestions for additional research, my reflections, and summarizing thoughts.

Overview of Study

The purpose of this qualitative pragmatic inquiry was to explore strategies used by IT satellite managers in the space industry to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks. The participants were current or prior contractors working for space agencies with experience in satellite operations and manufacturing. The geographical location of the study was the surrounding areas of Cape Canaveral, Florida. An essential criterion for participants was that they had experience working in the field relating to the research question. I used the ISTISM as the conceptual framework. Coding and interview transcriptions were performed using NVIVO software through which themes were discovered and documented. Implications for positive social change include the shift in focus for space agencies across the globe to (a) potentially clean space debris before crashing debris hurts those on Earth, (b) link several nations together with the goal of not generating space debris, and (c) utilize new technologies to prevent satellites from becoming weaponized.

Presentation of the Findings

The following research question guided this study: What strategies do IT satellite managers in the space industry use to properly harden and rapidly decommission satellites out of LEO if targeted by cyberattacks? I carried out semi-structured interviews with eight purposefully sampled participants to gather data with which to address the research question. With the implementation of purposeful sampling, researchers gain the capability to deliberately choose participants based on specific characteristics, thereby ensuring the collection of comprehensive and insightful data (Goodrich, 2019). I performed triangulation with a combination of industry document reviews, interviews, and observations provided by the interviewees. Some interviewees were able to share their firsthand experiences related to the semi-structured interview questions. All industry documents provided and participant comments were kept at the unclassified level. Member checking was performed to validate the collected data. I conducted interviews until I reached a point where new data did not yield additional insights or themes.

I coded with the data in NVIVO software from which three dominant themes emerged: (a) policy concerns, (b) system hardening/logistics and current decommissioning for IT satellites and supporting systems, and (c) legacy equipment. Additionally, two minor themes emerged (a) space laws/treaties gaps and (b) decommission methods.

My findings showed that IT satellite managers and space industry professionals are becoming more aware of potential cyberattacks against satellites and their supporting systems in LEO. The other findings indicated that IT satellite managers and space

industry professionals feel that there is a lack of clear-cut guidance regarding administrative polices to properly hardened systems against growing cyber security concerns. Cyber defense operations and decommissioning tactics exist but may not be considered rapid in nature due to the time delays in carrying out commands and receiving proper permissions from decision makers.

Major Theme 1: Policy Concerns

The participants interviewed had at least 5 years of experience in government or commercial support of space industry strategies, defensive cyber operations, and satellite communications. None of the participants were currently active-duty military, and they all had experienced a situation or exercised scenarios related to IT satellites, cyberattacks, and methods to decommission IT satellites or debris from LEO. I asked the participants the following semi-structured interview questions:

1. In your opinion, what different strategies would provide a better end result versus what is being used?
2. What administrative policies are in place to stop cyberattacks? Are they working?

Patterns and themes quickly presented themselves even though the participants worked for different contractors under varying space companies. Themes in patterns in one company were also discovered in other companies and government contractors in the space industry.

The first theme that presented itself was policy concerns regarding standardization across the space industry targeted at securing IT satellites. Policies play a crucial role in

the space industry for several reasons. Robust policies provide a regulatory framework that may establish guidelines for activities in space, ensuring safety, security, and the prevention of potential collisions (Melograna & Johnson, 2024). Space policies also help allocate and manage valuable resources and can be targeted towards facilitating responsible and sustainable use of space assets and their respective orbits. Additionally, policies may contribute to international collaboration by defining norms and standards and fostering cooperation among nations in space exploration and utilization. Space is being proliferated by numerous countries simultaneously, which expands the potential of space collisions. Regulations are essential for addressing issues, such as space debris mitigation, spectrum management, and liability, in the event of accidents or collisions. Robust policies in the space industry focused on IT satellites are critical for fostering a structured and organized environment that promotes diplomatic and effective utilization of outer space. Policies proving effective may be replicated in other satellite operations, such as GPS, weather, and research satellites, because they function similarly to IT satellites in communication technologies.

Participant 2 (P2) stated that the National Institute of Standards and Technology (NIST) consists of publications of baseline cybersecurity for companies and governments, and P1 and P3 mentioned that there are a lot of protocols in place and a lot of checks for the government sector, such as NASA. NIST plays a fundamental role in space operations by providing guidelines, standards, and best practices for ensuring the security, reliability, and interoperability of space systems and their associated technologies. NIST develops and maintains a wide range of standards and guidelines,

including those related to cybersecurity, encryption, data protection, and risk management, which are essential for securing space assets in orbit and their supporting ground infrastructure(s) (Zhu et al., 2022). By adhering to NIST standards, space agencies and IT satellite managers may enhance the resilience of their systems against cyber threats, ensure the integrity of their data and communications, and promote interoperability with other space systems and networks. NIST's work in developing and promoting standards for measurement, calibration, and instrumentation is necessary for guaranteeing the accuracy and reliability of space-based measurements and observations (Zhu et al., 2022). P3 summarized how NIST's contributions to space operations help to enhance the safety, security, and efficiency of space missions, ensuring that both ground and LEO assets can accomplish their objectives successfully while minimalizing the risks associated with potential cyberattacks. However, these policies are strictly targeted at government and government-backed/funded IT satellites with commercial space industries not falling within the same baseline requirements.

Ensuring the protection of commercial satellites is essential due to their critical roles in national security, economic vitality, and international relations. Commercial satellites also significantly contribute to a country's defense capabilities by providing critical communication, navigation, and surveillance functions (Melograna & Johnson, 2024) Any cyberattack and/or compromise of commercial satellite systems could jeopardize a nation's ability to respond effectively to security threats. P4 and P5 summarized that the chance that an economic impact due to disruptions or attacks on commercial satellites is substantial, affecting various industries and individuals who rely

on satellite services for communication, broadcasting, weather monitoring, and more. P6 stated that “GPS is embedded through timing signals and servers, cell phone towers. Much more than just navigation. Banking, you look at the atomic clock.” Mass panic could arise across the globe if communications were to fail from satellite collisions or cyber-attacks. P6 shared an experience of the mid-90s, when Motorola started to shut down because they did not have the required 24 satellites to maintain the coverage, which also led to issues with cell phone signals and timing issues. At this time, policies were not in place to treat outages or anomalies and cyberattacks.

Without strong policies to address satellite outages, anomalies, and cyberattacks, the consequences could be catastrophic. IT satellites play an integral role in critical functions, such as communication and national security. An absence of thorough policies may leave IT satellite systems vulnerable to disruptions, potentially leading to widespread communication breakdowns, compromised GPS services, inaccurate weather predictions, and compromised military operations. Moreover, without strict guidelines in place, the lack of accountability could exacerbate the impact of cyberattacks, potentially leading to data breaches, unauthorized access, and even sabotage of critical IT satellites. Without proactive policy measures to address these threats, IT satellites may become jeopardized, leading to the failure of satellite-dependent services and the weakening of global connectivity and security. The establishment of effectively strict and robust policies is imperative to safeguarding the integrity and functionality of satellite networks in an increasingly interconnected world.

Collaborative efforts to secure both commercial and government satellites are necessary for fostering stability, positive international relations, and sustained economic growth. Commercial satellite technology often drives advancements in space-related technologies, contributing to ongoing research and development and later replicated by governments once proven secure (Melograna & Johnson, 2024). Commercial satellite technology innovations may contribute to competitiveness on a global scale but also present dangers to government and military satellites currently in orbit. Commercial satellites may not be as restricted or locked down to the same policies as government and military satellites. P7 discussed that safeguarding commercial satellites helps prevent space debris, collisions, and other hazards, contributing to the long-term health and accessibility of outer space. The protection of commercial satellites through strict policies is not only a matter of economic interest but also vital for national security, international collaboration, technological progress, and the sustainable use of space resources. P7 stated that "the FCC can go back and look at some of their language to maybe revise on certain scenarios" while discussing the 5-year decommissioning policy published by the FCC. P5 mentioned that the policy is not being abided by because many satellites are still in orbit past their projected end-of-life date. The FCC's 5-year decommissioning policy may be challenging, especially if there are difficulties in monitoring and verifying whether satellite operators adhere to the specified guidelines.

One country, such as the United States, cannot dictate what another country does in space. P6 discussed a lack of coordination and alignment with international standards for satellite decommissioning, which could potentially pose challenges for addressing the

global issue of space debris. P6 continued to highlight how some policies are in their infancy stages with needed rewrites because some are being ignored. If a space policy such as the FCC's 5-year decommission guidelines is not clear or is subject to interpretation, it may lead to confusion among satellite operators, potentially resulting in noncompliance or disputes by those set to adhere to them.

Various technological advancements in satellite design and cyberattack methods may outpace existing decommissioning and cyber protection policies, resulting in the need for periodic updates to ensure relevance and efficacy. Recent industry documents such as NASA Inspector General reports highlight known discrepancies needing immediate attention. Moreover, P6 stated that Space Mission Force is "going through some iterations" and shared past experiences of working in benign operating locations where anomalies were treated as the sun or communications issues versus having the mindset that potential outages may be nefarious. At the time, P6 did not have clear-cut guidance or policy on how to conduct forensics on outages or potential nefarious cyberattacks. P1, P2, P3, P4, P5, P6, P7, and P8 all agreed that policy revisions are needed to create a stronger defense of space assets in LEO. Table 5 shows the frequency of occurrence of the theme policy.

Table 3

Frequency of First Theme

Major/minor themes	Count	References
Policy	12	57
Space laws/treaty	7	34

Due to space policies and treaties, the participants knew about various directives and treaties established and agreed that some are not being properly followed or have gaps requiring restructuring. All participants agreed that there were policies created to prevent space debris, increase global security, limit the potential for military escalation, lower collateral damage, address violations of international norms, and maintain the peaceful use of outer space. Efforts to address these concerns often involve advocating for responsible space behavior and international cooperation. More specifically, Space Policy Directive 3 was developed to promote collaboration with international partners to address common challenges related to space traffic management and debris mitigation (Gleason, 2020). Space Policy Directive 2 (SPD-2) was developed to streamline regulations and policies related to commercial space activities (Giannopapa & Antoni, 2023). SPD-2 called for a review of existing regulations that may hinder the growth of the commercial space industry and directs government agencies to revise or exclude rules that are considered unnecessary or overly burdensome. Moreover, SPD-2 mentioned that the Federal Aviation Administration should work collaboratively with the private sector to create a more conducive regulatory environment. According to P5, the rules being deemed unnecessary or overly burdensome may be placing IT satellites in harm's way by allowing private sectors to essentially bend rules and take advantage of gaps. P5 brought up the following scenario that may need to be written into SPD-2 or other policies, "If their lifespan, if they're trying to make these 25 years, what if these corporations and companies are no longer existent? What if they declare bankruptcy? What if they're no longer involved in this type of industry?" This potential scenario could become a major

issue as start-up space companies may not have the funding to continue space operations, and there is no clear guidance on who is responsible for removing unfunctional satellites. A country new to the space race could be considered in the same scenario if it no longer can decommission its own satellites from orbit. P5 stated that there is a need to pass statutes and laws where they are putting the responsibility on corporations with incentives in place to remove their debris because, at this time, there is no international space debris removal company.

Space debris in orbit poses a danger to IT satellites in orbit because if no one is monitoring them or decommissioning them properly, they could be highjacked and turned into projectiles targeted at other satellites or space stations. The time it takes for a satellite to naturally deorbit from LEO depends on various factors, which include the altitude of the orbit, the atmospheric density at that altitude, and the satellite's mass and size (Thayer et al., 2021). Without a proper or sanctioned interaction, satellites in LEO may take several years to decades to naturally deorbit due to lower atmospheric density. According to P5 and P7, satellites deorbiting naturally may pose a danger to the human population as they are uncontrolled and could potentially cause harm or damage. All participants agreed that satellite removal tools, such as ASAT weapons, are highly controversial from a policy perspective due to the associated risks and challenges.

P6 specifically highlighted that the intentional destruction of satellites during ASAT tests generates significant space debris, raising concerns about the sustainability of space activities. This is because debris poses risks to other operational satellites and the ISS and emphasizes the need for policies that address space debris mitigation and the

responsible use of space. Moreover, ASAT tests can contribute to the militarization of space, potentially leading to an arms race and heightened global security tensions. The development and testing of ASAT or rapid forced decommissioning methods other than self-destruct methods challenges existing international norms, to include the principles outlined in the Outer Space Treaty. This showcased a theme of the necessity for robust policies that promote peaceful and responsible behavior in outer space. Haphazardly testing ASAT technologies and rapid kinetic decommissioning tactics could raise tensions between nations as they generate space debris that would take years to deorbit naturally. Efforts to establish guidelines for testing ASAT weapons should be aimed at mitigating risks, encouraging international cooperation, and upholding the stability of space activities within a policy framework that prioritizes the deterrence of space debris and the peaceful use of outer space.

The ISTISM proposed by Hong et al. (2003) offers a holistic framework that can be applied and theoretically prove instrumental in addressing and rectifying cybersecurity policy issues within the space industry. ISTISM places emphasize the interconnectedness of various elements within a system. ISTISM satellites can be considered as a system for the application of ISTISM. Aligning the complex nature of cyber threats and policies to combat them could benefit the entire space domain. By applying ISTISM to cybersecurity policies, space industry stakeholders can better understand the interdependencies between different components of their systems, including satellites, ground stations, and communication link networks. The ISTISM lens may offer a perspective that enables the identification of potential vulnerabilities and points of entry

for cyber threats, allowing for the development of policies that encompass the entire space infrastructure.

Moreover, the ISTISM encourages a practical and adaptive approach to cybersecurity policy formulation or revision. Instead of relying solely on reactive measures, space industry leaders can employ proactive strategies based on a thorough understanding of how different components interact. Being proactive in attacking potential issues may lower the risk of Kessler syndrome taking place earlier due to cyber security attacks on IT satellites. Space professionals assigned to apply ISTISM can implement continuous monitoring, real-time analysis, and the integration of emerging technologies to enhance the resilience of space systems against evolving cyber threats. By incorporating Hong's ISTISM into cybersecurity policy frameworks, the space industry can adopt a more robust and strict security posture, better equipped to anticipate, prevent, and respond to cyber threats effectively. P4 highlighted that space agencies are looking to improve their effectiveness when countering cyber satellites in space or cyberattacks on satellites in space. P6 stated that top-level leaders' buy-in will be required as they need to see the importance of proactive approaches versus reactive actions against IT satellite cyber-attacks. P2 provided the same context and P6 mentioned tools such as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) but they rely on policy to know when to implement them as defensive cyber operations. IDS and IPS' serve similar yet distinct roles in cybersecurity. An IDS is used in a passive mode to monitor network or system activity while analyzing incoming traffic and identifying potential security threats or anomalies based on predefined rules or

intelligence-based threat signatures. When an intrusion or suspicious activity is detected, the IDS generates alerts or notifications to notify IT security personnel, allowing them to investigate and respond to the incident manually. On the other hand, IPS actively interferes with blocking or mitigating identified threats in real time through automated means. According to P2, IT satellite managers may employ proactive measures such as IPS to block malicious traffic, drop connection attempts, or reconfigure network settings. IPS seeks to prevent unauthorized access or malicious activities from compromising system confidentiality, integrity, and availability. While IDS focuses on detection and alerting, IPS takes preventive action to actively stop potential threats, which provides an additional layer of defense against cyberattacks (Kizza, 2024).

Defensive cyber operations have become increasingly vital for safeguarding satellites due to the growing reliance on satellite technology. With the proliferation of sophisticated cyber threats and the expanding number of IT satellites in LEO, the probability for malicious actors to disrupt or compromise satellite operations has considerably intensified. Effective defensive cyber operations are essential to proactively identify and mitigate cyber threats, ensuring the resilience and integrity of satellite systems against evolving and persistent cyber-attacks whether from insider threats, nation-state actors, or non-state actor organizations. A new series of U.S. Space Force (USSF) doctrine has been released that reflects on the growing recognition of space as a critical domain for national security and defense. As space becomes increasingly congested and also contested along with the proliferation of space debris the US has pursued the enhancements and abilities to defend its space assets and maintain its

strategic advantage in space. Defensive cyber operations play a very significant role in maintaining a strategic advantage and can be done through the USSF developing Mission Defense Teams (MDT). MDTs are groups of cyber professionals who get assigned specific or multiple space systems for penetration testing and hardening (Healey & Caudill, 2020). MDTs attempt to find vulnerabilities and potential exploitation before they can be used by those with malicious intentions. These groups of individuals break down space systems and analyze every connection, asset, and logistical support needed for them to operate. If anomalies are discovered, the teams detect, monitor, and report the findings to higher-level headquarters for deeper analysis (Vićić & Harknett, 2024). By establishing the USSF as the sixth military branch, the United States aims to consolidate and prioritize its space-related activities, resources, and expertise within a dedicated organization focused on space operations. The USSF is responsible for organizing, training, and equipping space forces to protect the United States and allied interests in space, ensuring that the United States maintains its leadership and dominance in this critical domain (Kostyuk, & Gartzke, 2024).

IT policies based on ISTISM would prioritize the development of redundancies and failover mechanisms to minimize the impact of hardware failures or cyberattacks. The developed policies may emphasize the importance of interoperability and standardization to facilitate continuous communication and coordination between satellites and ground stations in the event of potential cyber or known cyber anomalies. ISTISM could be deployed to encourage a holistic approach to cybersecurity, identifying that threats to one component of the system can have cascading effects on the entire

space network or clusters of satellites in LEO. IT policies developed from implementing ISTISM could prioritize proactive measures such as encryption, authentication, and IDS/IPS measures to safeguard satellite data and communication channels.

ISTISM highlights the importance of endless monitoring, feedback loops, and adaptation to evolving threats and technological advancements. If one encryption method or countermeasure is proving insufficient in monitoring results, IT satellite managers could change their procedures. IT policies for LEO satellites should incorporate mechanisms for real-time monitoring of system performance, anomaly detection, and rapid response to potential threats. By leveraging the principles of ISTISM, policymakers, and decision-makers can develop agile and adaptive IT policies that promote the resilience, reliability, and security of satellite networks in LEO. A rapid response procedure or response plan based on policy is vital in addressing cyberattacks on satellites due to the critical nature of their functions and the potential cascading impacts of compromised systems. A compromised system could become a lethal projectile in orbit causing more crashes which may ultimately start the Kessler syndrome phenomenon. A prompt and definitive response is necessary to contain cyber-attacks in order to mitigate their effects and prevent further exploitation of vulnerabilities. A successful attack on one IT satellite may be replicated and used again on another to introduce crimpling effects. Delayed or inadequate response could lead to prolonged disruptions in essential services, compromised data integrity, and a higher probability of follow-up attacks. Due to the interconnected nature of IT satellites means that a breach in one system can hypothetically spread across multiple satellites, amplifying the scope and

severity of the destruction. Rapid response measures that can continuously be revamped due to their development through detailed application of ISTISM could be essential to minimizing downtime, maintaining operational continuity, protecting the confidentiality, integrity, and availability of satellites, and limiting the potential of setting off Kessler Syndrome.

Major Theme 2: System Hardening/Logistics

All the participants spoke about the various methods used to harden systems against attacks within their control of IT satellite systems. The most recurring term that came up during system hardening is encryption. The second major and minor themes appeared which were IT satellite managers hardening systems including logistics and current decommissioning methods. Hardening IT satellites against cyber-attacks is essential due to their critical role in numerous aspects of human life on Earth. Any compromise of a satellite's confidentiality, integrity, or availability may have far-extensive consequences, disrupting not only communication and navigation but also potentially hindering emergency response efforts and jeopardizing national security (Yue et al., 2023). Safeguarding IT satellites against cyberattacks is necessary to maintain the reliability and functionality that human society heavily relies on.

Table 4

Frequency of the Second Theme

Major/minor themes	Count	References
System hardening	29	40
Decommission methods	12	27

P2 highlighted the interconnected nature of satellite networks and underscored the significance of securing them against cyber threats. A breach in one satellite system could potentially spread across multiple satellites, amplifying the scope and impact of the attack. If a scenario such as a satellite hijacking took place it could lead to widespread disruption of services and complicated efforts to restore normal operations. There are some dependencies on satellite technology that extend beyond civilian applications, such as military operations and intelligence gathering. An adversary could target IT satellite systems for espionage, sabotage, or strategic advantage. In order to deter or lower the potential for cyber-attacks, IT satellite managers deploy robust cybersecurity measures to protect sensitive military communications, surveillance capabilities, and Command and Control (C2) functions from exploitation or disruption. According to NASA documents, C2 technologies are fundamental for managing spacecraft operations, because they ensure the integrity and security of data transmissions and enable timely and precise command execution for satellite movements. In the NASA 2020 Collision Avoidance for Space Environment Protection in accordance with The National Aeronautics and Space Act, 51 U.S.C. § 20113 (a). The director highlighted the need for robust and resilient C2 systems to support the increasing complexity and demands of space missions, including those involving IT satellites in LEO. The NASA document also emphasized the importance of continuous innovation and adaptation of C2 technologies to address evolving threats, enhance mission flexibility, and improve overall mission success.

The ever-evolving cyber threats require nonstop vigilance and adaptation of security measures to counter emerging risks that exist on space and ground stations. As

adversaries change their attack vectors and styles, cyber security professionals must stay one step ahead and implement security measures to deter their actions. Cyber attackers are becoming more advanced, employing advanced techniques such as malware, phishing, and DoS attacks to exploit vulnerabilities in IT satellite systems (Niyonsaba et al., 2023). P2 highlighted that as satellites become more interconnected with terrestrial networks and Internet of Things (IoT) devices, they become susceptible to a wider array of cyber threats. P7 highlighted the necessity for space agencies to invest in comprehensive cybersecurity solutions tailored to the unique challenges posed by IT satellite systems. These systems face a mass of cyber threats, including unauthorized access, data breaches, and malicious attacks, which could compromise IT satellite confidentiality, integrity, and availability. By investing in cybersecurity solutions, space agencies can stay ahead of malicious actors and protect their IT satellite systems from potential vulnerabilities and attacks. These solutions may include implementing encryption techniques, intrusion detection systems, and access controls to safeguard sensitive data and prevent unauthorized access. Additionally, regular security audits and vulnerability assessments can help space agencies identify and mitigate potential risks, ensuring the resilience and security of their IT satellite systems (Plotnek, 2022).

Again, the main point brought up regarding hardening IT satellite systems was the utilization of the Triple Data Encryption Standard (3DES). 3DES is a widely deployed encryption algorithm used by IT satellite managers and is known for its strength and resistance to cyber-attacks. A new finding was that the FCC regulates satellite communications and may impose encryption requirements as part of licensing or

authorization processes for satellite operators to follow (Al-Roweilly, 2020). The FCC safeguards satellites by ensuring communications used by their owners adhere to certain security standards to protect against unauthorized access, interception, or tampering with data. A problem with this encryption requirement is that the United States and its allies may strictly adhere to this while other countries in the space race could potentially ignore FCC suggestions. Within United States-based organizations, the FCC may require satellite operators to implement encryption measures to protect sensitive information transmitted through satellite networks. Alongside the FCC, the National Telecommunications, and Information Administration (NTIA), and DoD are responsible for advising the President of the United States on telecommunications and information policy issues and are within the jurisdiction to issue guidelines or recommendations concerning encryption practices for satellite communications (Kirchhoff & Barkley, 2023). The NTIA also works intimately with federal agencies, space industry stakeholders, and other relevant entities to develop policies that promote the security and resilience of IT satellite systems and their networks.

Hardening satellites in LEO through 3DES can play a crucial role in securing data transmissions between satellites and ground stations, as well as within satellite systems themselves (Dyer et al., 2023). (P8) summarized that it is just as crucial to protect ground stations, along with actual satellites in space. Moreover, the findings showed that logistical aspects are considered in hardening satellites such as ensuring the integrity of their fabrication, transportation, set-up, launch, and control. By utilizing 3DES encryption, IT satellite operators can ensure that sensitive information, such as command

signals, telemetry data, and mission-critical communications, remains confidential and protected from interception by unauthorized parties. P1 stated that by employing encryption potential adversaries will hear and see gargled communications. 3DES encryption standard adds a layer of security that is exceptionally critical for satellite networks operating in the inherently vulnerable environment of space, where interception and tampering risks are heightened.

3DES encryption can increase the resilience of IT satellite systems against cyber threats and attacks (Janardhan & Neelima, 2024). IT satellites operating in LEO are exposed to a diversity of potential adversaries that are seeking to exploit vulnerabilities for purposes such as espionage, and sabotage, so strong encryption mechanisms such as 3DES are vital for safeguarding against unauthorized access and manipulation of satellite operations. 3DES encryption helps mitigate the risk of data breaches and unauthorized command injections by rendering intercepted or tampered data unreadable without the decryption key. 3DES ensures the integrity and authenticity of data exchanged between satellites and ground stations, which fortifies the overall security posture of satellite networks against cyber threats (Samanth & Balachandra, 2022).

The longevity and widespread adoption of 3DES encryption make it a rational choice for protecting satellites in LEO, where reliability and compatibility are cardinal considerations. While newer encryption algorithms such as Advanced Encryption Standard (AES) offer superior performance and security features, many legacy systems and satellite platforms may still rely on 3DES due to its proven track record and interoperability with existing infrastructure. By leveraging 3DES encryption, satellite

operators can achieve a balance between integrity, confidentiality, availability, compatibility, and performance. 3DES ensures the continued resilience and effectiveness of IT satellite systems currently operating in the dynamic and challenging environment of LEO. (P8) addressed the need to implement physical security measures, such as tamper-resistant hardware, secure facilities, and restricted access controls, to protect satellites from physical tampering or sabotage attempts. The findings showed that there are countermeasures in place to prevent insider threats but require levels of verification to ensure they are effective. P7 shared that it is crucial to secure storage facilities and stringent access controls mitigate the risk of unauthorized individuals gaining physical access to satellite components or infrastructure.

Advanced Encryption Standard (AES) is another encryption method that can be used to secure IT satellite communications against compromise (Pirzada et al., 2020). AES is a symmetric encryption algorithm broadly used to safeguard sensitive data in various applications, including IT satellite operations. AES operates on fixed-size blocks of data (128, 192, or 256 bits) and uses a series of substitution and permutation steps (substitution-permutation network) to encrypt and decrypt sensitive data (Qasaimeh et al., 2021). AES is vastly regarded for its security, efficiency, and widespread adoption in both civilian and military applications. By encrypting data using AES, IT satellite managers can ensure that unauthorized individuals cannot intercept or decipher the data, which allows them to maintain the confidentiality, integrity, and availability of satellite operations (Aissaoui et al., 2023). AES encryption is exceptionally valuable for securing telemetry data, command signals, and software updates sent to IT satellites, which

protects them from eavesdropping or tampering-based attacks during transmission. IT satellites operating in LEO may be susceptible to various forms of interference and exploitation attacks. According to P6, implementing AES encryption helps mitigate the risk of unauthorized access and manipulation of satellite operations. By encrypting data at rest and in transit, IT satellite managers can protect crucial information and ensure that satellite systems remain secure and fully equipped to fight ever-evolving cyber threats.

Through reviewing industry documents, Space Doctrine Publication (SDP) 4-0, titled "Sustainment," was discovered which outlined the principles and practices for sustaining space operations and capabilities. The publication emphasized the magnitude of sustainment in ensuring the effectiveness, resilience, and longevity of all space systems. SDP 4-0 directly highlighted the need for a comprehensive sustainment strategy that incorporates logistics, maintenance, personnel, and infrastructure to support space missions effectively (Blore, 2024). SDP 4-0 emphasized the vital role of logistics in sustaining space operations which aligned with P8's answers. The document discussed the importance of maintaining a robust supply chain to ensure the timely delivery of critical components and resources to space systems which may help deter weaknesses in cyber components. The publication also emphasized the need for effective inventory management, transportation, and distribution systems to support space missions in various operational environments.

Maintenance is another key focus of SDP 4-0, as it is vital to implement regular inspections, repairs, and upgrades to ensure the operational readiness of IT space systems and their controlling ground systems. The publication underlined the need for proactive

maintenance practices to prevent system failure and compromise. It also discusses the importance of incorporating maintenance considerations into the design and development of space systems to facilitate easier maintenance and repairs. Moreover, personnel and infrastructure are also key components of sustainment outlined in SDP 4-0. The publication emphasizes the importance of training and equipping personnel to effectively operate and maintain IT satellite systems and their controlling ground station. It also discussed the need for strong infrastructure, including facilities, communication networks, and support systems, to support space missions effectively. A weakness in one component could result in adversaries gaining unauthorized access to compromise IT satellites or their ground stations. SDP 4-0 presents a comprehensive framework for sustainment in space operations, with a clear emphasis on logistics, maintenance, personnel, and critical infrastructure in ensuring the effectiveness and longevity of space systems. Securing supply chain management is another tactic used to secure IT satellites during their development, creation, shipping, and launch. Ensuring the integrity and security of the supply chain for IT satellite components and software is essential for preventing the introduction of malicious hardware, counterfeit assets, or unapproved software into satellite systems and their control base stations (Varadharajan & Suri, 2023). Based on information gathered from P8, supply chain security measures implemented depend on rigorous inspections including vendor vetting, component authentication, purchasing audits, and secure manufacturing processes, help mitigate the risk of supply chain attacks targeting IT satellites.

P2 highlighted that regular software and firmware updates are used to harden IT satellites in LEO, alongside the computers used to second control signals and monitoring. Regularly updating satellite software and firmware with security patches may lower the vulnerabilities and minimize the risk of exploitation by cyber attackers or adversaries. Through timely updates, IT satellite managers can help ensure that satellite systems remain resilient against evolving threats and growing attack techniques. Firmware updates for satellites are necessary for maintaining the functionality, security, and performance of these assets in LEO. Findings show that updates are typically transmitted from ground control stations to satellites through established and encrypted communication links. Ground control personnel prepare the firmware update package, which includes firmware files, instructions for installation, and validation mechanisms to ensure integrity and authenticity (Falas et al., 2021). Satellite operators schedule the deployment of firmware updates based on operational requirements and coordinate with other ground stations or satellite networks to avoid interference with critical operations.

Updating an IT satellite at the wrong time without proper coordination could cause potential losses in communication or hinder the ongoing operations of an organization relying on the satellite going through firmware updates. During firmware installation, a satellite may reboot certain systems, but protocols may be implemented to transfer control to redundant components or enter safe mode to minimize disruptions. After completing the installation process, the satellite will likely perform additional verification and validation checks in order to confirm the successful application of the update and proper system functionality.

There was evidence of the participants sharing their knowledge on quick response measures when a cyberattack may be happening on their IT satellites. This became apparent because all the participants shared that there are no rapid decommissioning methods currently in place. According to P1, past methods of using mechanical arms to decommission IT satellites are becoming a thing of the past as manned flights are as frequent to repair satellites in LEO. The rate and cost of satellites have drastically changed since the early days of satellite deployments. Dedicated spacecraft or missions can still be launched to actively remove dead satellites or space debris from LEO. These manned missions normally involve catching the targeted satellite or debris by means of robotic arms, nets, or harpoons, and then either deorbiting them using propulsion or directing them towards atmospheric reentry. P7 shared that it takes multiple layers of approval to truly decommission a satellite and have it exhausted its last amount of fuel to burn in the Earth's atmosphere or be pushed into the graveyard orbit. P7 continued on in-depth about satellites being equipped with propulsion systems that allow for their maneuvering into lower orbits, where atmospheric drag accelerates their decay and eventual reentry into the Earth's atmosphere. This propulsion system is a current decommissioning method that allows for controlled deorbiting, permitting operators to target specific reentry locations and minimize the risk of debris endangering populated areas.

The new finding was discussed by all participants of the tactic of shutting off satellite capabilities as a defensive measure to prevent hijacking or cyber compromise. P1 used the term bricking a satellite as a means to prevent the infiltration of a satellite, but it

comes with its own dangers. Bricking a satellite can prevent cyberattacks by effectively disconnecting it from communication networks and isolating it from potential attackers. When a satellite is powered off, its systems, including communication interfaces and command channels, are deactivated, making it unavailable to external entities attempting to infiltrate or compromise its components. By shutting off an IT satellite, operators can mitigate the risk of cyberattacks targeting vulnerabilities in satellite software, firmware, gaps in encryption, or communication protocols (Pavur & Martinovic, 2022). Simply powering off an IT satellite allows operators to conduct thorough security assessments through forensics in order to apply necessary software patches or updates and implement remediation measures to address identified vulnerabilities. The decision to power down an IT satellite enhances the overall security posture of the satellite system if it is experiencing anomalies. Nonetheless, it is important to note that shutting off a satellite may disrupt satellite-dependent services and operations, so this approach should be carefully planned and executed to minimize potential impacts on critical functions. The satellite needs to be properly configured to be shut down by its owners and not from potential vulnerabilities that can be exploited to cause a shutdown by adversaries.

ISTISM can be applied to the implementation of 3DES encryption methods for IT satellites in LEO by considering the interconnectedness and interdependencies within the IT satellite systems. According to IST, intricate systems like satellite networks entail various interconnected components that function together to achieve specific objectives. Applying IST to 3DES encryption methods would involve recognizing the interaction between hardware, software, communication protocols, and cybersecurity measures

within the satellite system. ISTISM can be applied to tactics used to utilize emergency shutdown procedures for IT satellites in LEO. In order to do this policymakers and satellite engineers should consider how the shutdown process affects different components of the satellite system. This is because it would involve recognizing the relationship between physical hardware, controlling software, communication links, and operational capabilities within the satellite system. Based on interviews with participants, none of them had to carry out shutdown procedures for a satellite due to cyber anomalies. However, the ISTISM application could allow satellite operations to integrate emergency shutdown protocols into satellite control systems and enable them to conduct regular drills and simulations as if a real attack were taking place. Exercising cyberattacks through drills and simulations would allow IT, and satellite managers, to refine procedures based on lessons learned from previous incidents or near-misses.

ISTISM stresses the need for holistic and integrated approaches to cybersecurity. When implementing 3DES encryption methods for IT satellites in LEO, policymakers and engineers should consider how encryption fits into the expansive ecosystem of satellite operations. Many satellite constellations operate differently with various ground stations, operating systems, and controlling policies. Applying ISTISM may showcase the need to not only encrypt data transmissions but also harden satellite hardware, software, and communication channels to create a thorough defense against cyber threats. Again, ISTISM points out the importance of interoperability and compatibility which may be beneficial for IT satellites in operation and those projected for future launch. When deploying 3DES encryption across satellite networks, it is vital to ensure that

encryption protocols are compatible with existing satellite hardware and software. A lack of proper planning could introduce problems in the future if not caught in time. This requires coordination between IT satellite manufacturers, operators, and cybersecurity experts to develop standardized encryption protocols that can be seamlessly integrated into satellite systems without disrupting current operations. The cost to retrofit current IT satellites may be a hefty price but would aid in the prevention of compromise and the potential danger of satellite hijacking.

Finally, ISTISM stresses the need for continuous monitoring, feedback loops, and adaptation to evolving threats and advancements in technology. When implementing 3DES encryption methods for IT satellites in LEO, it is essential to establish mechanisms for real-time monitoring of encryption performance, anomaly detection, and rapid response to potential threats. Although all cyberattacks cannot be predicted, implementing strong countermeasures may decrease the potential of a targeted attack being successful. Employing encryption methods for communications is a strong baseline to limit the number of compromises. This would involve integrating encryption monitoring tools into satellite ground control systems and establishing protocols for analyzing encryption-related data to identify and address vulnerabilities proactively. By applying the principles of ISTISM to 3DES encryption methods, policymakers and engineers can generate robust and resilient cybersecurity strategies to protect IT satellites in LEO from cyber threats effectively.

Major Theme 3: Legacy Equipment

The third and final theme that was identified was the growing concern on legacy or outdated equipment that is still in orbit. All participants spoke on a growing concern of legacy or outdated satellite and launch components in LEO and spoke on how difficult they could be to retrofit or protect due to obsolete and non-supported technologies. It became apparent during the interviews that there are no rapid decommission procedures to address legacy equipment in LEO. According to all participants, legacy and outdated satellites that remain in LEO can contribute to the growing problem of space debris. Defunct, non-operational, or outdated IT satellites are at risk of colliding with active satellites, other space debris, or even manned spacecraft. Legacy equipment generates significant hazards to operational missions and the safety of astronauts and cosmonauts. Space debris collisions can generate additional debris, which further exacerbates the space pollution problem and increases the risk of future collisions in the cascading effect of Kessler syndrome.

Table 5

Frequency of Third Theme

Major/minor themes	Count	References
Legacy equipment	8	29

P5 shared a valid concern that was also shared by P7 regarding IT satellites becoming legacy or outdated due to company shutdown. If a company launches satellites and afterwards goes out of business, it can have substantial repercussions on both the operational integrity of the satellite and other satellites in LEO. With the absence of financial and operational support of IT satellites essential functions such as maintenance,

monitoring, and communication with the satellites may conclude. This can lead to a gradual degradation of IT satellite systems over time in LEO, which increases the risk of malfunctions, collisions, and operational failures with no one on console to report the errors. A failure to have a responsible entity to manage the satellites no longer being maintained, monitored, or communicated with allows them to theoretically become uncontrolled objects in LEO. Uncontrolled objects in LEO pose grave hazards to other operational satellites and contributing to the growing issue of space debris which may set off the Kessler syndrome phenomenon. A loss of communication with these satellites may impact services dependent on them, such as telecommunications, and scientific research. The potential scenario of unsupported IT satellites in LEO due to company collapses underscores the importance of effective regulatory oversight, accountable satellite stewardship, and contingency planning in order to lessen the risks of uncontrolled assets in space. All participants agreed that outdated space assets need to be removed from orbit before they may become compromised due to their limited technologies to defend themselves and that leaving them in orbit to naturally decay or deorbit is just adding to the space pollution issue.

Aging space technologies that become legacy or outdated present a danger due to their increased likelihood of failure, which can result in malfunctions, collisions or compromise which could lead to the generation of more space debris. As IT satellites and spacecraft age, the components, software, and materials used in their construction may degrade or become less reliable, leading to an elevated risk of operational anomalies or overall complete failures. These failures can result in the satellite becoming unresponsive

or uncontrollable, posing hazards to other operational satellites, current or future crewed spacecraft, and other satellites in LEO. The 2020 Defense Space Strategy highlights the U.S. government's desired conditions and strategic objectives for the next 10 years to combat identified threats, challenges, and expand on opportunities. The 2020 Defense Space Strategy focuses on four primary goals (a) maintain awareness of the space environment, (b) enhance U.S. space capabilities, (c) deter aggression in space, and (c) promote responsible behavior in space. The strategy emphasizes the importance of integrating space capabilities into military operations, enhancing resilience against threats, and strengthening partnerships with allies and commercial entities. The strategy also highlights the need for sustained leadership and investment in space to support national security objectives aligning with comments made by P7.

P5 highlighted that even a power outage or spike should be investigated as a potential cyber anomaly since all the systems are integrated and adversaries could potentially be using targeted attacks to compromise IT satellites. Inspecting a power spike on an IT satellite as a cyber-anomaly is critical because it could indicate a cyber-attack or unauthorized interference. While power spikes can occur due to various factors, including hardware malfunctions or environmental conditions, they can also be a sign of malicious activity by adversaries. Investigating a power spike in the context of an IT satellite's operational environment and looking for indicators of malicious activity, such as unusual network traffic or unauthorized access, can help determine if the spike was caused by a cyberattack. Treating a power issue as a potential cyber anomaly enables IT satellite managers to take proactive measures to investigate the event, mitigate any

potential damage, and enhance the overall satellite's cybersecurity. By responding swiftly to potential cyber threats, IT satellite managers can protect critical infrastructure and assets, ensuring the confidentiality, integrity, and availability of systems on the ground and in LEO. This approach may align with cybersecurity best practices set by space industries and militaries which emphasize the importance of detecting and responding to cyber threats to safeguard against unauthorized access and malicious activity.

Legacy IT satellites or aging components within them may lack modern features and capabilities to effectively mitigate risks and respond to emerging cyber-attacks. Older IT satellites may not be equipped with advanced encryption, propulsion systems, collision avoidance technologies, or systems for safe deorbiting at the end of their operational life. These potential gaps can increase the probability of collisions or the creation of new space debris, contributing to the growing issue of space congestion and the risk of the Kessler syndrome phenomenon. Older IT satellite technologies may be more susceptible to cyber threats and hacking attempts due to outdated software, inadequate security measures, and vulnerabilities that have emerged over time. Cyber-attacks targeting aging satellites can compromise their confidentiality, integrity, and availability potentially leading to unauthorized access, hijacking, data breaches, or malicious manipulation of satellite daily procedures. As the dependence on space-based assets for critical functions continues to grow, the risks associated with aging space technologies become progressively concerning. (P6) highlighted the need for proactive measures to address these challenges and safeguard the long-term sustainability and safety of space activities within LEO and other orbits.

Various components of an IT satellite are likely to become outdated, largely due to technological advancements and evolving space requirements. Onboard computers and processors are significant components that may become obsolete as advances in microelectronics and computing technology lead to more powerful and energy-efficient processors. Communication systems, including transponders, antennas, and modems, are prone to obsolescence as communication technologies evolve rapidly, making aged IT satellite systems less efficient or compatible with modern standards. IT satellite antennas can be hijacked, though it is a complex and challenging process for the individual or group with malicious intentions. Hijacking IT satellite antennas would likely involve gaining unauthorized access to the antenna's control systems or communication protocols. Nation-state or non-state actors may attempt to exploit vulnerabilities in the antenna's software, firmware, or network connections in order to gain unauthorized control. Once an IT satellite antenna becomes hijacked, the attackers could potentially manipulate its pointing direction, frequency settings, or transmission power to disrupt legitimate satellite communications or redirect signals to unauthorized recipients igniting a man-in-the-middle (MitM) attack. MitM cyber-attacks can lead to service disruptions, data interception, or unauthorized access to sensitive information transmitted via satellite (Riggs et al., 2023). Older antennas on IT satellites in LEO may not be able to be retrofitted or upgraded quickly so satellite managers may need to consider replacement versus upgrading legacy components.

Countermeasures to prevent MitM on IT satellites in LEO may involve implementing strong encryption, and authentication mechanisms, such as AES and 3DES

to protect data transmitted between satellites and ground stations against being intercepted or modified by attackers (Rogers, 2022). With encryption, IT satellite managers ensure that even if an attacker intercepts the data, they cannot decipher its contents without the encryption key. In addition, employing mutual authentication between satellites and ground stations can prevent unauthorized entities from posing as legitimate parties. Mutual authentication ensures that both parties verify each other's identity before exchanging sensitive information, reducing the risk of MitM attacks. IT satellite managers can use secure communication protocols, such as TLS (Transport Layer Security), to further enhance the security of IT satellite communications in LEO. TLS can be used to encrypt data transmitted over the network and provide authentication to ensure the integrity and confidentiality of the communication. By using TLS, IT satellite managers can protect against eavesdropping, tampering, and imitation attacks. Furthermore, implementing IDS and IPS technologies may help detect and allow cybersecurity professionals to respond to suspicious activities or unauthorized access attempts. Strong encryption enables IT satellite managers to take measures to prevent MitM. All participants mentioned that a vital aspect of encryption methods would be the use of regular security audits and recurring vulnerability assessments in order to identify and mitigate potential security risks, ensuring the continued security and integrity of IT satellites in LEO.

ISTISM provides a framework for understanding the complex interrelationships and dependencies within satellite networks, making it applicable to the identification of legacy and outdated satellites in LEO. ISTISM can be applied to emphasize the

connectedness of satellite systems, where various components, including orbital parameters, telemetry data, and ground-based observations, need to cooperate in sync to achieve successful space operations. Applying IST to satellite identification involves recognizing the whole satellite ecosystem, and the possibility of collisions in LEO. IT satellite managers can leverage multiple sources of data and information to accurately identify legacy and outdated satellite systems to plan for their removal in a structured manner.

ISTISM emphasizes the significance of studying the interaction between different elements within the satellite system. When identifying legacy and outdated satellites in LEO, it is essential to understand how these IT satellites interact with other assets in orbit, such as active satellites, space debris, and natural orbital drag. This can be achieved through analyzing orbital dynamics, trajectory data, and telemetry information to differentiate between target satellites and other objects in the surrounding area. Knowing the age of an asset in space is crucial for estimating its end of life. ISTISM also emphasizes the need to align with stakeholders and key decision-makers to make them aware of the issue and gather buy-in. P6 spoke on the necessity of gathering stakeholder buy-in to make proactive suggestions a reality to lower the need for reactive measures. Replacing satellites often may be pricey but it may prevent the possibility of large amounts of end-of-life assets orbiting in LEO. IT satellite managers can use identification efforts to benefit from the collective expertise, resources, and data sharing among satellite operators, space industry agencies, research institutions, and international organizations. By establishing standardized protocols and information-sharing mechanisms,

stakeholders can streamline the identification process, improve data accuracy, and enhance the overall effectiveness of satellite tracking and monitoring efforts. Decommission IT satellites that are outdated and no longer serve a purpose should be decommissioned to prevent the growth of space pollution.

Again, ISTISM highlights the importance of continuous monitoring and adaptation to evolving challenges and as new technologies are created, older technologies become legacy. As the satellite environment in LEO evolves, with new satellites launched and existing satellites reaching the end of their operational life, it's essential to develop adaptive strategies for identifying legacy and outdated satellites. This can be done by leveraging advanced technologies such as Machine Learning, Artificial Intelligence (AI), and predictive analytics to analyze vast amounts of data and identify patterns or anomalies indicative of legacy satellites. P2 highlighted AI and predictive analysis and how they can significantly enhance the defense of IT satellites from cyber-attacks by providing advanced threat detection, automated response capabilities, and proactive security measures. AI algorithms can analyze vast amounts of data from IT satellite systems, ground stations, and network traffic very quickly in order to identify patterns and anomalies indicative of cyberattacks (Diro et al., 2024). IT satellite managers can leverage machine learning and deep learning techniques to detect suspicious activities, such as unauthorized access attempts, malware infections, or unusual behavior that may indicate a potential cyber threat. Predictive analysis can help anticipate and mitigate potential cyber-attacks by evaluating historical data, security trends, and threat intelligence to identify potential vulnerabilities and weak points in IT

satellite systems. IT satellite managers can potentially forecast cyber-attack vectors and vulnerabilities based on threat intelligence and lessons learned from other satellite operators in the space industry. AI-driven automated responses can facilitate IT satellites quickly and effectively responding to cyber threats in real time. AI systems can autonomously detect and neutralize threats, such as malware or unauthorized access attempts, without human intervention, helping to minimize the impact of cyber-attacks and ensure the continued operation of satellite operations. Through industry documentation research, a December 2020 NASA Spacecraft Conjunction Assessment and Collision Avoidance Best Practices Handbook was collected that highlights how NASA will work in integration with the military to protect space assets. The Best Practices Handbook states that automation such as AI and machine learning will become more used as the number of space assets grows requiring a need for faster processing (Martin & Freeland, 2021). AI and machine learning will go hand in hand to both protect satellites from being compromised and deter potential collisions through predictive analysis.

Clear and truthful documentation of assets in space could allow stakeholders to be aware of what is becoming end-of-life within their Area of Responsibility (AOR). Applying ISTISM would require attention to detail and calls for feedback loops and iterative improvement. By collecting and analyzing data from previous identification efforts, stakeholders can refine their methodologies, update their algorithms, and enhance their capabilities for identifying legacy and outdated satellites in LEO. An iterative approach may ensure that identification techniques remain effective and adaptable to

changing conditions, eventually contributing to the long-term sustainability and safety of space operations for all space agencies.

Applications to Professional Practice

The specific IT problem was that some IT satellite managers in the space industry lack strategies to properly harden and rapidly decommission satellites out of LEO if targeted by cyber-attacks. The participants provided their strategies used to maintain IT satellite operations in their fields which allowed for the identification of three dominant themes (a) policy concerns, (b) system hardening/logistics and current decommissioning for IT satellites and supporting systems, and (c) legacy equipment. Additionally, two minor themes emerged (a) space laws/treaties gaps and (b) decommission methods. All the participants expressed how crucial satellite operations were for humans on Earth for daily tasks, military operations, and scientific research. Due to the ever-increasing threat of cyberattacks against IT satellites, space agencies, and satellite managers must be prepared to take proactive measures to deter threats. If proactive measures are not taken, IT satellite systems may fall victim to cyber-attacks which could ultimately lead to the catastrophic phenomenon known as Kessler syndrome. All space agencies, industries, and Nations that utilize satellites in LEO require current information on the challenges of properly hardening IT satellites against cyberattacks, limiting the proliferation of space debris, and policies in place to keep space safe for everyone. Furthermore, strategies and lessons learned/best practices from one space industry can be beneficial to the deployment of new IT satellites in LEO. I drew from ISTISM which provided a framework to identify tactics that can be implemented by decision makers to revise and

strengthen policies, procedures for space debris removal, and methods to keep IT satellite hardening baselines current. The answers received from the participants were very similar with the same areas of concern and aligned with strategic industry documents/military doctrine. The findings showcased that even though there are policies and strategies in place, there are significant gaps in the verbiage. Additional resources could be used to develop and implement rapid decommissioning methods targeted at removing IT satellites affected by cyberattacks. The same rapid decommission methods could also be used to address the growing concern of space debris which could aid in the reduction of legacy IT satellites in LEO as well as other orbits.

Policy was the major theme running throughout this study and was discussed by every participant. To minimize the potential for IT satellite attacks, IT satellite managers could ensure the assets under their control properly adhere to FCC policies and implement robust encryption standards to deter cyber-attacks. Space debris could be lowered and limited by properly following the FCC's guidelines for decommissioning satellites after five years of operation. Continuous wavier extensions and lack of concern to remove IT satellites reaching end-of-life in LEO are generating a web of space assets that could potentially set off the Kessler syndrome phenomenon. There is no set date for when the Kessler syndrome could happen but as more satellites and debris are placed into orbit without others being removed the likelihood of the phenomenon rises. Key leaders and decision makers within the space industry need to place higher levels of concern into proactive measures before emergency reactive measures are needed to address IT satellite cyberattacks and collisions. The cost of reactive measures may heavily outweigh the

costs of proactive measures and be too late to address space debris if it gets out of hand. It is important to note that the participants themselves could not share details of potential cyberattack avenues on their systems due to classification.

The findings revealed that strategies employed to harden IT satellites against cyber-attacks were consistent across the industry, focusing primarily on encryption and intrusion monitoring. Encryption techniques, such as AES and 3DES were widely used to protect sensitive data transmitted to and from satellites, ensuring its confidentiality, integrity, and availability. Intrusion monitoring systems were also commonly deployed to detect and respond to unauthorized access attempts or malicious activities targeting satellites' IT systems. These strategies reflect the industry's recognition of the importance of cybersecurity in safeguarding satellite operations and data against cyber threats.

My study highlighted the potential benefits of collaboration and information sharing among space industry professionals and space agencies to enhance defensive cyber operations on IT satellites. By working together, industry stakeholders can leverage their collective expertise and resources to develop and implement more effective cybersecurity strategies and measures. Collaborative efforts can also facilitate the sharing of best practices, threat intelligence, and lessons learned, enabling satellite operators to strengthen their cybersecurity posture and better protect their assets in space. ISTISM underscored the importance of implementing testing and recurring feedback loops to validate the effectiveness of both existing and newly developed cybersecurity strategies. Regular testing and evaluation can help identify vulnerabilities, assess the impact of new threats, and refine cybersecurity measures to address emerging challenges. By

incorporating ISTISM principles into their cybersecurity practices, satellite operators can ensure that their IT satellites remain secure and resilient in the face of evolving cyber threats.

The final finding of the study highlighted the awareness among all participants regarding the growing concern about legacy equipment and the continued use of older technologies on assets within LEO. This awareness highlights the need for proactive measures to address the risks associated with legacy equipment, such as implementing upgrades, applying security patches, and conducting regular maintenance. By addressing these challenges, satellite operators can enhance the reliability and security of their satellite systems and mitigate the risks posed by aging technologies. Another key finding emphasized the importance of cataloging and monitoring existing space debris for tracking purposes. Sharing the locations of space debris is crucial to ensuring that all space industries understand what is in their potential path and can take preventive measures to avoid collisions. This collaborative approach is essential for preventing the Kessler syndrome, a scenario in which the density of objects in LEO is high enough to trigger a cascade of collisions, leading to a significant increase in space debris and posing a serious threat to satellites and spacecraft. Additionally, space agencies across the globe can leverage AI algorithms to analyze vast amounts of data from IT satellite systems, ground stations, and network traffic rapidly. By using AI for cybersecurity purposes, space agencies can identify patterns and anomalies indicative of cyber-attacks, enabling them to respond quickly and effectively to potential threats. This application of AI aligns with the principles of ISTISM, which emphasizes the importance of continuous

monitoring and adaptation to evolving challenges. As new technologies are created, older technologies become a legacy, highlighting the need for adaptive strategies to address emerging threats and ensure the resilience of IT satellite systems.

Implications for Social Change

Strengthening policies for satellite management, securing the defense cyber operations of IT satellites in LEO, and removing outdated/legacy equipment from space has significant implications for social change. Improved policies for IT satellite management can lead to more efficient and sustainable use of space resources, benefiting society as a whole. Space industries must be proactive versus reactivate when it comes to deterring the growth of space pollution and having strong strategies and countermeasures to prevent IT satellite compromise is a key component. Through the establishment of clear guidelines for IT satellite deployment, operation, and disposal, policymakers and decision-makers can reduce the risk of the Kessler syndrome phenomenon ultimately ensuring the long-term viability of space. This can lead to a more secure and sustainable space environment, which is essential for supporting future space exploration, scientific research, and commercial activities.

This study may be seen by space industry professionals and agencies focusing on efforts to better protect their assets in space. Securing the defense cyber operations of IT satellites in LEO is crucial for protecting critical infrastructure and daily capabilities that humans rely on. As society becomes increasingly dependent on satellite technology for communication, navigation, weather forecasting, and military operations, we as a human population must ensure the security and integrity of satellite systems in LEO. The focus

of LEO can be expanded to other orbits as well as being essential to protect for future space operations. Strengthening defensive cyber operations measures can mitigate the risk of cyber-attacks that could disrupt or compromise satellite operations, leading to potential disruptions in vital services on Earth. This stresses the importance of proactively investing in cybersecurity capabilities and technologies to protect satellite systems from evolving cyber threats and ensuring other nations uphold and adhere to space regulations, guidelines, and treaties to ensure space is useful for every nation in the future.

Furthermore, removing outdated/legacy equipment from space can contribute to the overall safety and sustainability of space activities (Manulis et al., 2021). If space becomes overrun with pollution from collisions of IT satellites and other space debris, we will be limiting the potential for future space exploration. Legacy IT satellites and current/future debris pose a risk of collisions with active satellites, increasing the amount of space debris and the potential for Kessler syndrome. This study highlighted the need to eliminate outdated equipment from space, which could be built upon by space agencies and operators to reduce the risk of collisions, making space activities safer and more sustainable for future generations. This can also pave the way for future space missions and activities by clearing up valuable orbital space for new communications satellites, manned space stations, and other space technologies without the worry of them being compromised or destroyed by debris.

In conclusion, this study will indirectly have a constructive influence on strengthening policies for satellite management, securing the defensive cyber operations

of satellites in LEO, and removing outdated/legacy equipment from space have wide-ranging implications for social change. These efforts can lead to a more sustainable, secure, and efficient use of space resources, benefiting society by ensuring the continued availability of critical services and infrastructure that rely on satellite technology. By addressing these challenges, policymakers, decision makers, space agencies, and satellite operators across the globe can contribute to a protected, more sustainable, and more safeguarded space environment for future generations.

Recommendations for Action

The study encompassed participants from various space agencies, all united by the common goal of safeguarding their IT satellites in LEO. While the focus was predominantly on internal strategies within their respective organizations, rather than the broader space industry, there was a clear consensus on the need for IT satellite managers to thoroughly review their policies. This includes identifying and addressing any indefinite or unclear areas that may require additional context.

One key recommendation stemming from the study is for decision-makers and key leaders to adhere to the FCC's recommendation of a five-year decommissioning timeline. This measure aims to reduce the proliferation of legacy IT satellites in LEO, thereby enhancing the overall security posture of satellite constellations.

Another crucial aspect highlighted in the study is the importance of empowering lower to mid-level IT satellite managers. These managers are often the subject matter experts with the most current hands-on experience. Therefore, they should have a clear voice and the freedom to express their viewpoints without fear of reprisal. This approach

can help prevent misunderstandings or misrepresentations of their expertise when higher-level leaders are briefed on their behalf.

Given the increasing threat of cyberattacks against IT satellites in LEO, space agencies are advised to conduct thorough analyses of their hardening procedures. Additionally, they should focus on enhancing supply chain management practices and implementing rigorous hiring/background investigation protocols to mitigate insider threats. Furthermore, allocating more funding toward defensive cyber operations tools is recommended to strengthen overall cybersecurity defenses for IT satellites in LEO.

Recommendations for Further Study

I cannot state the results are generalized across the entire space industry; this study can be built upon by other researchers completing a quantitative study using a large number of participants from other space agencies/industries outside of the Eastern Florida region. Moreover, the quantitative results could be used for mixed-method studies in the future. A quantitative study may allow future researchers to apply statistical tools in order to analyze the gathered data to predict outcomes, causes, effects, and strategies of IT satellite decommissioning methods. A limitation of this study was that some topics could not be discussed because of their classification level and most participants stated there has not been an overwhelming need to rapidly decommission satellites. Further studies can be directed at the strategies to remove IT satellites from LEO in a rapid manner to calculate the effectiveness of their decommission without generating space debris. Future studies could validate the steps needed to rapidly decommission IT satellites out of LEO and identify the strategies and their gaps for immediate fix actions. The results from this

study could be disseminated to other researchers tackling the same or similar research questions to develop a deeper understanding of rapidly decommissioning IT satellites.

I recommend other countries study the relationship between rapidly decommissioning IT satellites and the deterrence of unnecessary space debris. During the interviews, there were comments made that the United States seems to be the front runner and most concerned about tracking and generating space debris, yet the Kessler syndrome would be a global catastrophe. In an ever-evolving space domain, it would be essential to know how other countries are operating in space to deter the unnecessary generation of space debris and their strategies to de-clutter space to cut down space pollution for all humankind. These results could generate a best practice guide or globally accepted strategy for all countries involved in space operations to adhere to. Furthermore, new countries becoming part of the space race could also rely on the best practices to deter the unnecessary generation of space debris from the beginning.

Reflections

My study focused on preventing cyberattacks on IT satellites in LEO and came with a multitude of challenges that required perseverance and resilience. First, the complex and constantly evolving nature of cybersecurity demanded a deep understanding of both theoretical principles and practical applications. I personally benefited from extensive research and analysis of strategies and countermeasures against potential threats. Additionally, the interdisciplinary nature of the subject, combined aspects of computer science, engineering, and innovative space technologies which require me to navigate a wide range of complex concepts and methodologies.

Perseverance played a crucial role in overcoming these challenges and completing multiple interviews when I believed it was going to be difficult to find participants willing to share their experiences. Thankfully my chair was there to offer essential feedback to address setbacks and obstacles. Moreover, the ever-changing technologies within cybersecurity meant that I needed to remain adaptable and willing to reassess approaches and new developments mentioned during interviews. My personal biases of what technologies could be the most secure needed to be repressed to ensure I did not conflict with the data gathered. I am thankful to have completed this portion of the study and made every effort to ensure biased opinions were not included in the collection of data or its analysis. Again, perseverance was essential to me as a researcher to see it through to completion and make meaningful contributions to the field of cybersecurity for IT satellites in LEO and social change. I hope that my findings will be the ignition needed for IT satellite managers and other space professionals to further the study and potential application of rapid decommissioning tactics that can be used to remove IT satellites from LEO which may be affected by cyber-attacks ultimately lowering the potential of Kessler syndrome.

Summary and Study Conclusions

Current strategies for decommissioning IT satellites from LEO represent a multifaceted challenge, especially considering the rising concerns regarding sophisticated cyber-attacks on space assets. The urgent need to implement rapid capabilities may become critical in this context as space becomes a potential battlespace. It is essential to conduct a thorough analysis of existing strategies, doctrines, and best practices, with the

buy-in of decision makers and stakeholders, to ensure that any vagueness or vulnerabilities are addressed and removed. While one space agency may have robust security measures in place, others may lag behind, potentially exposing their IT satellites to cyber-attacks, hijacking, or other compromises that could contribute to the undesirable Kessler syndrome phenomenon. In addition to enhancing security measures, there is also a need for a broader societal change regarding space cybersecurity. This includes fostering international cooperation and standardization of cybersecurity practices across space agencies and satellite operators to protect manned missions in space and future space missions. Furthermore, public awareness and engagement regarding the implications of cyberattacks on space assets are crucial for ensuring the sustainability and security of space operations. By addressing these challenges and promoting social change, we can better protect IT satellites in LEO from cyber threats and mitigate the risk(s) associated with space proliferation.

References

Adeyeye, Y. O. (2020). *Power, people, places, and spaces: examining the politics of participation across scales of resource governance* [Doctoral dissertation, University of British Columbia]. https://doi.org/10.14288/1.0391066

Adushkin, V. V., Aksenov, O. Y., Veniaminov, S. S., Kozlov, S. I., & Tyurenkova, V. V. (2020). The small orbital debris population and its impact on space activities and ecological safety. *Acta Astronautica*, *176*, 591-597. https://doi.org/10.1016/j.actaastro.2020.01.015

Aglietti, G. S., Taylor, B., Fellowes, S., Salmon, T., Retat, I., Hall, A., Chabot, T., Pisseloup, A., Cox, C., Zarkesh, A., Mafficini, A., Vinkoff, N., Bashford, K., Bernal, C., Chaumette, F., Pollini, A., & Steyn, W. H. (2020). The active space debris removal mission RemoveDebris. Part 2: In-orbit operations. *Acta Astronautica*, *168*, 310–322. https://doi.org/10.1016/j.actaastro.2019.09.001

Ai, Y., Cui, X., & Yuan, D. (2022). Key technologies of real-time location service in satellite navigation and positioning network based on Internet of things. *Computational Intelligence and Neuroscience*, 1–12. https://doi.org/10.1155/2022/5191871

Ailor, W. (2022). Protecting the LEO environment. *Journal of Space Safety Engineering*. *9*(3), 449-454. https://doi.org/10.1016/j.jsse.2022.07.001

Aissaoui, R., Deneuville, J. C., Guerber, C., & Pirovano, A. (2023). A survey on cryptographic methods to secure communications for UAV traffic

management. *Vehicular Communications*. *44* (1), 2214-2096 https://doi.org/10.1016/j.vehcom.2023.100661

Ajupov, A., Sherstobitova, A., Syrotiuk, S., & Karataev, A. (2019). The risk-management theory in modern economic conditions. *E3S Web of Conferences, 110*, 02040. EDP Sciences. https://doi.org/10.1051/e3sconf/201911002040

Akasaka, Y., Takasaka, S., Sugizaki, R., Guo, C., & Vasilyev, M. (2022). S-band amplifier using highly nonlinear fibers. *2022 27th OptoElectronics and Communications Conference (OECC) and 2022 International Conference on Photonics in Switching and Computing (PSC)*, 1–3. https://doi.org/10.23919/OECC/PSC53152.2022.9850030

Alewine, H. C. (2020). Space accounting. *Accounting, Auditing & Accountability Journal*, *33*(5), 991-1018. https://doi.org/10.1108/AAAJ-06-2019-4040

Alhazmi, A. A., & Kaufmann, A. (2022). Phenomenological qualitative methods applied to the analysis of cross-cultural experience in novel educational social contexts. *Frontiers in Psychology*, *13*, 1495. https://doi.org/10.3389/fpsyg.2022.785134

Al-Roweilly, S. (2020). *Laws and regulations for the new telecommunications Services: A global survey of law, policy, and emerging technology*.

Amiri, A. K., Cavusoglu, H., & Benbasat, I. (2015). Enhancing strategic IT alignment through common language: Using the terminology of the resource-based view or the capability-based view? *Thirty Sixth International Conference on Information Systems*, 1–12. https://core.ac.uk/download/pdf/301367416.pdf

Anderson, J., & Eppard, J. (1998). Van Kaam's method revisited. *Qualitative Health Research*, *8*(3), 399-403. https://doi.org/10.1177/104973239800800310

Assumpção, J. J., Campos, L. M., Vazquez-Brust, D. A., & M. Carvalho, M. (2023). The orchestration of green supply chain management practices to enable performance measurement and evaluation. *Production Planning & Control*, 1-20. https://doi.org/10.1080/09537287.2023.2214526

Azad, A., Sernbo, E., Svärd, V., Holmlund, L., & Björk Brämberg, E. (2021). Conducting in-depth interviews via mobile phone with persons with common mental disorders and multimorbidity: The challenges and advantages as experienced by participants and researchers. *International Journal of Environmental Research and Public Health*, *18*(22), 11828. https://doi.org/10.3390/ijerph182211828.

Babchuk, W. A. (2019). Fundamentals of qualitative analysis in family medicine. *Family Medicine and Community Health*, *7*(2), 1–10. https://doi.org/10.1136/fmch-2018-000040

Bai, S., Wang, W., Chen, Z., & Yao, W. (2021). Research on abnormal output current drop of solar array of a low earth orbit satellite. *IEEE Aerospace and Electronic Systems Magazine*, *36*(5), 48–58. https://doi.org/10.1109/maes.2020.3043137

Barato, F. (2022). Comparison between different re-entry technologies for debris mitigation in LEO. *Applied Sciences*, *12*(19), 1–40. https://doi.org/10.3390/app12199961

Bartos, O. J., & Wehr, P. (2002). *Using conflict theory*. Cambridge University Press.

Bateman, A. (2022). Mutually assured surveillance at risk: Anti-satellite weapons and cold war arms control. *Journal of Strategic Studies*, *45*(1), 119–142. https://doi.org/10.1080/01402390.2021.2019022

Bearman, M. (2019). Focus on methodology: Eliciting rich data: A practical approach to writing semi-structured interview schedules. *Focus on Health Professional Education: A Multi-Professional Journal*, *20*(3), 1-11. https://doi.org/10.11157/fohpe.v20i3.387

Bergen, N., & Labonté, R. (2020). "Everything is perfect, and we have no problems": Detecting and limiting social desirability bias in qualitative research. *Qualitative Health Research*, *30*(5), 783–792. https://doi.org/10.1177/1049732319889354

Bhangu, S., Provost, F., & Caduff, C. (2023). Introduction to qualitative research methods - Part I. *Perspectives in Clinical Research*, *14*(1), 39–42. https://doi.org/10.4103/picr.picr_253_22

Bianchi, G., Montaruli, M. F., Roma, M., Mariotti, S., Di Lizia, P., Maccaferri, A., Facchini, L., Bortolotti, C., & Minghetti, R. (2022). A new concept of transmitting antenna on bi-static radar for space debris monitoring. *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–5. https://doi.org/10.1109/ICECCME55909.2022.9988566

Blore, A. T. (2023). Responsiveness is not operational. *Æther: A Journal of Strategic Airpower & Spacepower*, *2*, 45-58.

Boddy, K., Cowan, K., Gibson, A., & Britten, N. (2017). Does funded research reflect the priorities of people living with Type 1 diabetes? A secondary analysis of research questions. *BMJ Open, 7*(9), e016540. https://doi.org/10.1136/bmjopen-2017-016540

Boley, A. C., & Byers, M. (2021). Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere, and on Earth. *Scientific Reports*, *11*(1), 10642. https://doi.org/10.1038/s41598-021-89909-7

Bowers, L. (2022). To the moon: Application of an alternative funding policy for the U.S. Space Force. *Public Contract Law Journal*, *51*(3), 467–488. https://www.americanbar.org/groups/public_contract_law/publications/public_contract_law_jrnl/51-3/to-moon-application-an-alternative-funding-policy-the-us-space-force/

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201-216. https://doi.org/10.1080/2159676X.2019.1704846

Brewer, E., Lin, J., & Runfola, D. (2022). Susceptibility & defense of satellite image-trained convolutional networks to backdoor attacks. *Information Sciences*, *603*, 244–261. https://doi.org/10.1016/j.ins.2022.05.004

Bromiley, P., & Rau, D. (2016). Missing the point of the practice-based view. *Strategic Organization*, *14*(3), 260-269. https://doi.org/10.1177/1476127016645840.

Brookin, J. (2019, April 30). SpaceX satellites will fly low to prevent space junk. *WIRED*. https://www.wired.com/story/spacex-satellites-orbital-altitude/#:~:text=SpaceX%20has%20received%20Federal%20Communications%20Commission%20approval%20to,to%20provide%20high-speed%2C%20low-latency%20broadband%20around%20the%20world

Budhu, J. A., Velazquez, A. I., Said, R. R., & Jordan, J. T. (2021). Opinion & special articles: maximizing inclusiveness and diversity through virtual residency applications and interviews. *Neurology*, *97*(13), 647-650. https://doi.org/10.1212/WNL.0000000000012487

Burns, K., & Turchak, L. (2007). Sputnik - Why the Russians were first in space. *AIAA SPACE 2007 Conference & Exposition*, 1–13. https://doi.org/10.2514/6.2007-6063

Bush, A. A., & Amechi, M. H. (2019). Conducting and presenting qualitative research in pharmacy education. *Currents in Pharmacy Teaching and Learning*, *11*(6), 638-650. https://doi.org/10.1016/j.cptl.2019.02.030

Butina, M. (2015). A narrative approach to qualitative inquiry. *American Society for Clinical Laboratory Science, 28*(3), 190-196. https://doi.org/10.29074/ascls.28.3.190

Carcary, M. (2020). The research audit trail: Methodological guidance for application in practice. *Electronic Journal of Business Research Methods*, *18*(2), pp166-177. https://doi.org/10.34190/JBRM.18.2.008

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Cartis, T., Smuleac, A., Pascalau, R., & Simon, M. (2021). Realization and increase the density of points for the Geodetic Network by G.N.S.S. measurements in the U.A.T. Zarand. *Research Journal of Agricultural Science*, *53*(4), 30–37. https://rjas.ro/download/paper_version.paper_file.924cbcccc5a197bb.4361727469732e706466.pdf

Caskurlu, S., Richardson, J. C., Maeda, Y., & Kozan, K. (2021). The qualitative evidence behind the factors impacting online learning experiences as informed by the community of inquiry framework: A thematic synthesis. *Computers & Education*, *165*(104111), 1–19. https://doi.org/10.1016/j.compedu.2020.104111

Chen, B., Yim, S. I., Kim, H., Kondabathini, A., & Nuqui, R. (2020). Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications. *IEEE Transactions on Power Systems*, *36*(1), 592-602. https://doi.org/10.1109/TPWRS.2020.3022588

Chen, Z., Zhang, J. M., Sarro, F., & Harman, M. (2023). A comprehensive empirical study of bias mitigation methods for Machine Learning classifiers. *ACM Transactions on Software Engineering and Methodology*, *1*(1), 1–13. https://doi.org/10.48550/ARXIV.2207.03277

Chou, Y. C., Ma, X., Wang, F., Ma, S., Wong, S. H., & Liu, J. (2022). Towards sustainable multi-tier space networking for LEO satellite constellations. *2022*

IEEE/ACM 30th International Symposium on Quality of Service (IWQoS). https://doi.org/10.1109/IWQoS54832.2022.9812872

Church, S. P., Dunn, M., & Prokopy, L. S. (2019). Benefits to qualitative data quality with multiple coders: Two case studies in multi-coder data analysis. *Journal of Rural Social Sciences*, *34*(1), 2. https://egrove.olemiss.edu/jrss/vol34/iss1/2

Cloutier, C., & Ravasi, D. (2021). Using tables to enhance trustworthiness in qualitative research. *Strategic Organization*, *19*(1), 113-133. https://doi.org/10.1177/1476127020979329

Cojocari, I., Meier, M., Laurent, P., Laviron, A., Arrigucci, M., Carminati, M., Deda, G., Fiorini, C., Geigenberger, K., Glas, C., Greiner, J., Hindenberger, P., King, P., Lechner, P., Losekamm, M., Mertens, S., Meßmann, D., Rückerl, S., Toscano, L., … Willers, M. (2023). Calorimeter calibration of the ComPol CubeSat gamma-ray polarimeter. *Nuclear Instruments & Methods in Physics Research. Section A, Accelerators, Spectrometers, Detectors and Associated Equipment*, *1046*. https://doi.org/10.1016/j.nima.2022.167662

Coleman, P. (2022). Validity and reliability within qualitative research for the caring sciences. *International Journal of Caring Sciences*, *14*(3), 2041-2045. https://oro.open.ac.uk/81588/

Crane, L. (2018). The arms race in space. *New Scientist*, *238*(3173), 22–23. https://doi.org/10.1016/s0262-4079(18)30655-9

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(1), 1–9. https://doi.org/10.1186/1471-2288-11-100

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal*, *8*(4), 273–289. https://doi.org/10.1046/j.1365-2575.1998.00040.x

Daubner, L., Buhnova, B., & Pitner, T. (2023). Forensic experts' view of forensic-ready software systems: A qualitative study. *Journal of Software: Evolution and Process*. https://doi.org/10.1002/smr.2598.

Dawson, L., & Dawson, L. (2018). A Summary of the US Space Program and Its Relationship to the Military. *War in Space: The Science and Technology Behind Our Next Theater of Conflict*, 61-86. https://doi.org/10.1007/978-3-319-93052-7_5

DeJonckheere, M., & Vaughn, L. M. (2019). Semi-structured interviewing in primary care research: A balance of relationship and rigor. *Family Medicine and Community Health*, *7*(2), 1–8. https://doi.org/10.1136/fmch-2018-000057

Dilworth, S. W., & Osborne, D. D. (2022). Cyber threats against and in the Space Domain: Legal remedies. *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, 235–247. https://doi.org/10.23919/CyCon55549.2022.9811057

Diro, A., Kaisar, S., Vasilakos, A. V., Anwar, A., Nasirian, A., & Olani, G. (2024). Anomaly detection for space information networks: A survey of challenges,

techniques, and future directions. *Computers & Security*, *139*. https://doi.org/10.1016/j.cose.2024.103705

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, *20*(5). https://doi.org/10.7748/nr2013.05.20.5.28.e327

Dorji, P., & Tenzin, J. (2021). Application of Kagan's cooperative learning structures to maximize student engagement: An action research. *Journal of Education, Society and Behavioral Science*, *34*(3), 54-64. https://doi.org/10.9734/jesbs/2021/v34i330317

Du, B., Liu, F., Sun, X., Song, R., & Wang, L. (2021). A prediction method of LEO satellite orbit control effect based on multiple regression analysis model. In *2021 Global Reliability and Prognostics and Health Management (PHM-Nanjing)*, 1–6. https://doi.org/10.1109/PHM-Nanjing52125.2021.9612824

Dunstan, J. E. (2013). Space trash: Lessons learned (and ignored) from Space Law and Government. *Journal of Space Law*, *39*, 23. https://airandspacelaw.olemiss.edu/wp-content/uploads/2020/07/JSL-39.1.pdf

Dyer, C. S., Ryden, K. A., Morris, P. A., Hands, A. D., Mcnulty, P. J., Vaille, J. R., ... & Xapsos, M. A. (2023). The Living With a Star Space Environment Testbed Payload. *IEEE Transactions on Nuclear Science*, *70*(3), 200-215. https://doi.org/10.1109/TNS.2023.3239734

Egeli, S. (2021). Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability. *Journal*

for Peace and Nuclear Disarmament, *4*(1), 116-140. https://doi.org/10.1080/25751654.2021.1942681

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security*, *19*(3), 243-256. https://doi.org/10.1016/S0167-4048(00)88613-7

Eriksson, J., & Giacomello, G. (2022). Cyberspace in space: Fragmentation, vulnerability, and uncertainty. In *Cyber Security Politics* (pp. 95-108). Routledge. https://doi.org/10.4324/9781003110224-8

Falas, S., Konstantinou, C., & Michael, M. K. (2021). A modular end-to-end framework for secure firmware updates on embedded systems. *ACM Journal on Emerging Technologies in Computing Systems*, *18*(1), 1-19. https://doi.org/10.1145/3460234

Falco, G. (2020). When satellites attack: Satellite-to-satellite cyber-attack, defense and resilience. In *ASCEND 2020* (p. 4014). https://doi.org/10.2514/6.2020-4014

Falduto, M., & Peeters, W. (2022). Trade-off approach for launching smallsats. *New Space*. https://doi.org/10.1089/space.2022.0003

Feng, W., Xiu-luo, L., Jia, W., Yao, L., Gang, A., & Long-fei, C. (2020). Research on space transportation intelligence control. In *2020 International Conference on Computer Engineering and Intelligent Control (ICCEIC)*, 271–274. https://doi.org/10.1109/ICCEIC51584.2020.00058

Feng, X., & Behar-Horenstein, L. (2019). Maximizing NVivo utilities to analyze open-ended responses. *The Qualitative Report*, *24*(3), 563-572.

Fernandez, L., Ruiz-de-Azua, J. A., Calveras, A., & Camps, A. (2020). Evaluation of LoRa for data retrieval of ocean monitoring sensors with LEO satellites. *IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium*, 359–362. https://doi.org/10.1109/IGARSS39084.2020.9324377

Ferrer, R. A., & Ellis, E. M. (2019). Moving beyond categorization to understand affective influences on real-world health decisions. *Social and Personality Psychology Compass*, *13*(11), 1–16. https://doi.org/10.1111/spc3.12502

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry: QI*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont Report? *The American Journal of Bioethics, 17*(7), 15–21. https://doi.org/10.1080/15265161.2017.1329482

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 19–32. https://doi.org/10.5590/josc.2018.10.1.02

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

Gerson, K., & Damaske, S. (2020). *The science and art of interviewing*. Oxford University Press.

Giannopapa, C., & Antoni, N. (2023). Space traffic management and its dual use: Space security strategies and cooperation in Europe. *Acta Astronautica*. https://doi.org/10.1016/j.actaastro.2023.01.038

Giri, D. V., Hoad, R., & Sabath, F. (2020). *High-power radio frequency effects on electronic systems*. Artech House.

Gleason, M. P. (2020). Establishing space traffic management standards, guidelines and best practices. *Journal of Space Safety Engineering*, *7*(3), 426-431. https://doi.org/10.1016/j.jsse.2020.06.005

Goodrich, A. (2019). Spending their leisure time: Adult amateur musicians in a community band. *Music Education Research,* 1–11. https://doi.org/10.1080/14613808.2018.1563057

Grant, R. M. (1996). Toward a knowledge-based theory of the firm: Knowledge-based Theory of the Firm. *Strategic Management Journal*, *17*(S2), 109–122. https://doi.org/10.1002/smj.4250171110

Groh, J. (2022, December 15). SpaceX set to shatter launch record. *USA Today*.

Guo, R., Cai, L., & Fei, Y. (2019). Knowledge integration methods, product innovation, and high-tech new venture performance in China. *Technology Analysis and Strategic Management*, *31*(3), 306–318. https://doi.org/10.1080/09537325.2018.1500688

Gupta, B., & Rathore, E. (2019). United nations general assembly resolutions in the formation of the outer space treaty of 1967. *Astropolitics*, *17*(2), 77–88. https://doi.org/10.1080/14777622.2019.1636633

Häder, D. P. (2021). Dumping of toxic waste into the oceans. In *Anthropogenic pollution of aquatic ecosystems* (pp. 353–371). Springer International Publishing. https://doi.org/10.1007/978-3-030-75602-4_16

Hakobyan, G., & Yang, B. (2019). High-performance automotive radar: A review of signal processing algorithms and modulation schemes. *IEEE Signal Processing Magazine*, *36*(5), 32–44. https://doi.org/10.1109/msp.2019.2911722

Halawa, M. G., Abdel-Aziz, Y., & Youssef, M. (2020). Analysis of close approach and collision probability between operational satellites and/or space debris. *INCAS Bulletin*, *12*(3), 113–127. https://doi.org/10.13111/2066-8201.2020.12.3.9

Han, C., Liu, A., Huo, L., Wang, H., & Liang, X. (2020). Anti-jamming routing for internet of satellites: A reinforcement learning approach. *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2877–2881. https://doi.org/10.1109/ICASSP40776.2020.9052911

Haralambous, H., Paul, K. S., & Gulyaeva, T. L. (2022). Topside investigation over Cyprus and Russia using Swarm data. *2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC)*, 1–4. https://doi.org/10.23919/AT-AP-RASC54737.2022.9814222

Harrison, T., Johnson, K., Moye, J., & Young, M. (2020). *Space threat assessment 2020*. Center for Strategic & International Studies.

Hassan, J., & Davenport, C. (2022, February 3). When the International Space Station retires, it will plunge into the ocean to die, NASA says. *The Washington Post*.

https://www.washingtonpost.com/science/2022/02/03/nasa-international-space-station-decommission-2031-ocean/

Healey, J., & Caudill, S. (2020). Success of persistent engagement in cyberspace. *Strategic Studies Quarterly*, *14*(1), 9-15.

Hemmler, V. L., Kenney, A. W., Langley, S. D., Callahan, C. M., Gubbins, E. J., & Holder, S. (2022). Beyond a coefficient: An interactive process for achieving inter-rater consistency in qualitative coding. *Qualitative Research*, *22*(2), 194-219. https://doi.org/10.1177/1468794120976072

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2016). Code saturation versus meaning saturation. *Qualitative Health Research, 27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Hitchens, T. (2019). Space traffic management: US military considerations for the future. *Journal of Space Safety Engineering*, *6*(2), 108-112. https://doi.org/10.1016/j.jsse.2019.04.003

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

Hori, K., Katsumi, T., Sawai, S., Azuma, N., Hatai, K., & Nakatsuka, J. (2019). HAN-Based Green Propellant, SHP163–Its R&D and Test in Space. *Propellants, Explosives, Pyrotechnics*, *44*(9), 1080-1083. https://doi.org/10.1002/prep.201900237.

Hou, Z., Li, Q., Foo, E., Dong, J. S., & de Souza, P. (2022). A digital twin runtime verification framework for protecting satellite systems from cyber-attacks. In *2022 26th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 117–122. https://doi.org/10.1109/ICECCS54210.2022.00022

Huang, L., Qu, Y., & Wang, J. (2022). Space debris removal ground-based laser nudge DE-orbiting system and modelling process. In *2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 478–483. https://doi.org/10.1109/ITAIC54216.2022.9836552

Husband, G. (2020). Ethical data collection and recognizing the impact of semi-structured interviews on research respondents. *Education Sciences*, *10*(8), 1–12. https://doi.org/10.3390/educsci10080206

Ignatovski, M. (2021). *Contributing factors to the number of individuals impacted by data breaches in healthcare organizations* [Doctoral dissertation, Capitol Technology University].

Jambak, M. I. (2015). The context of knowledge in organizations from resource-based theory to knowledge-based theory: A conceptual review. *Jurnal Sistem Informasi (JSI)*, *7*(1), 774–780. https://www.academia.edu/13225256/The_Context_Of_Knowledge_In_Organizations_From_Resource_Based_Theory_To_Knowledge_Based_Theory_A_Conceptual_Review

Janardhan, M. D., & Neelima, G. (2024). Implementation of Data Encryption and Decryption Technique using Graph Theory. *Journal of Engineering Sciences*, *15*(02). https://jespublication.com/uploads/2024-V15I02042.pdf

Ji, S., Zhou, D., Sheng, M., & Li, J. (2021). Mega satellite constellation system optimization: From a network control structure perspective. *IEEE Transactions on Wireless Communications*, *21*(2), 913-927. https://doi.org/10.1109/TWC.2021.3100247

Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, *24*(4), 602–611. https://doi.org/10.2307/2392366

Johansson, V., Soekadar, S. R., & Clausen, J. (2017). Locked Out. *Cambridge Quarterly of Healthcare Ethics, 26*(4), 555. https://doi.org/10.1017/S0963180117000081

Johnson, D., Scheitle, C. P., & Ecklund, E. H. (2021). Beyond the in-person interview? How interview quality varies across in-person, telephone, and Skype interviews. *Social Science Computer Review*, *39*(6), 1142-1158. https://doi.org/10.1177/0894439319893612

Johnson, J., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 1–22. https://doi.org/10.5688/ajpe7120

Johnson, R., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26. https://doi.org/10.3102/0013189x033007014

Kabay, M. E. (1996). *NCSA guide to enterprise security*. McGraw-Hill Companies.

Kasi, N. A., & Sallah, S. (2021). Inflation as a parent of unemployment: Revisiting the effects of unemployment and inflation on the economy of Pakistan under Karl Marx's conflict theory. *Pakistan Study Centre*, *13*(1), 88–101.

Kawamoto, S., Nagaoka, N., Sato, T., & Hanada, T. (2020). Impact on collision probability by post-mission disposal and active debris removal. *The Journal of Space Safety Engineering*, *7*(3), 178–191. https://doi.org/10.1016/j.jsse.2020.07.012

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2), 1–10. https://doi.org/10.1177/2059799120937242

Khoa, B. T., Hung, B. P., & Hejsalem-Brahmi, M. (2023). Qualitative research in social sciences: Data collection, data analysis and report writing. *International Journal of Public Sector Performance Management*, *12*(1-2), 187-209. https://doi.org/10.1504/IJPSPM.2023.132247

Khurelbaatar, L., Tumenjargal, T., Tumendemberel, B., Myagmar, O., Gollapudi, S., Omura, I., & Dashdondog, E. (2023). Space radiation induced failure rate calculation method using energy deposition probability function for high-voltage semiconductor device. *Materials Today. Communications*, *35*. https://doi.org/10.1016/j.mtcomm.2023.105499

Kirchhoff, A., & Barkley, T. (2023). Public Interest Comment for the National Telecommunications and Information Administration (NTIA) on the Initiative to

Protect Youth Mental Health, Safety and Privacy Online. *The Center for Growth and Opportunity*. https://www.thecgo.org/wp-content/uploads/2023/11/CGO-NTIA-RFC-KOS.pdf

Kizza, J. M. (2024). System intrusion detection and prevention. In *Guide to computer network security* (pp. 295-323). Springer International Publishing. https://doi.org/10.1007/978-3-031-47549-8_13

Knott, E., Rao, A. H., Summers, K., & Teeger, C. (2022). Interviews in the social sciences. *Nature Reviews. Methods Primers*, *2*(73), 1–15. https://doi.org/10.1038/s43586-022-00150-6

Kobayashi, M. M., Stocklin, F., Pugh, M., Kuperman, I., Bell, D., El-Nimri, S., Johnson, B., Huynh, N., Kelly, S., Nessel, J., Svitak, A., Williams, T., Linton, N., Arciaga, M., & Dissanayake, A. (2019). NASA's high-rate Ka-band downlink system for the NISAR mission. *Acta Astronautica*, *159*, 358–361. https://doi.org/10.1016/j.actaastro.2019.03.069

Koga, K., & Fukui, Y. (2022). Deorbiting of satellites by a free-flying space robot by combining positioning control and impedance control. *2022 22nd International Conference on Control, Automation and Systems (ICCAS)*, 965–971. https://doi.org/10.23919/ICCAS55662.2022.10003688

Kopeć, R. (2018). Space deterrence: In search of a 'magical formula.' *Space Policy*, *47*, 121–129. https://doi.org/10.1016/j.spacepol.2018.10.003

Kostyuk, N., & Gartzke, E. (2024). Fighting in cyberspace: Internet access and the substitutability of cyber and military operations. *Journal of Conflict Resolution*, *68*(1), 80-107. https://doi.org/10.1177/00220027231160993

Krajcovic, S., Silha, J., & Durikovic, R. (2020). AGO70: The Slovak space debris observations capability. *2020 New Trends in Signal Processing (NTSP)*, 1–5. https://doi.org/10.1109/NTSP49686.2020.9229540

Krause, J. (2021). The ethics of ethnographic methods in conflict zones. *Journal of Peace Research*, *58*(3), 329–341. https://doi.org/10.1177/0022343320971021

Krenn, A., Stewart, M., Mitchell, D., Dixon, K., Mierzwa, M., & Breon, S. (2019). Flight servicing of Robotic Refuelling Mission 3. *Space Cryogenics Workshop*. https://ntrs.nasa.gov/api/citations/20190027566/downloads/20190027566.pdf

Kucklick, J. P., & Müller, O. (2021). A comparison of multi-view learning strategies for satellite image-based real estate appraisal. *arXiv preprint arXiv:2105.04984*. https://doi.org/10.48550/arXiv.2105.04984

Kuwahara, T., Pala, A., Potier, A., Shibuya, Y., Sato, Y., Fujita, S., Suzuki, D., & Kaneko, T. (2022). Orbital demonstration of gossamer structure shape estimation using time-of-flight camera system. In *2022 IEEE/SICE International Symposium on System Integration (SII)*, 882–886. https://doi.org/10.1109/SII52469.2022.9708770

La Bella, J. (2021). Star Wars: Attack of the anti-satellite weapons in anticipatory self-defence. *University of the Pacific Law Review*, *52*(3), 733–759.

https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1364&context=uoplawreview

Lalbakhsh, A., Pitcairn, A., Mandal, K., Alibakhshikenari, M., Esselle, K. P., & Reisenfeld, S. (2022). Darkening low-earth orbit satellite constellations: A review. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 24383–24394. https://doi.org/10.1109/access.2022.3155193

LaMar, S., Gosselin, J. J., Happel, L., & Jayasumana, A. (2022). Combating advanced persistent threats for imminent low earth orbit cognitive communications systems. *2022 IEEE International Systems Conference (SysCon)*, 1–6. https://doi.org/10.1109/SysCon53536.2022.9773932

Le Billon, P. (2001). The political ecology of war: natural resources and armed conflicts. *Political geography*, *20*(5), 561-584. https://doi.org/10.1016/S0962-6298(01)00015-4

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. *Human resource development review*, *19*(1), 94-106. https://doi.org/10.1177/1534484320903890

Li, H., Shi, D., Wang, W., Liao, D., Gadekallu, T. R., & Yu, K. (2022). Secure routing for LEO satellite network survivability. *Computer Networks*, *211*. https://doi.org/10.1016/j.comnet.2022.109011

Li, H., Zong, Q., & Zhang, X. (2022). Anti-collision trajectory planning for satellite formation reconstruction based on deep reinforcement learning. *2022 41st*

Chinese Control Conference (CCC), 4672–4677. https://doi.org/10.23919/CCC55666.2022.9901660

Li, T., Higgins, J. P. T., & Deeks, J. J. (2019). Collecting data. In *Cochrane handbook for systematic reviews of interventions* (pp. 109–141). Wiley. https://doi.org/10.1002/9781119536604.ch5

Li, X., Sun, G., Kuang, Z., & Han, S. (2022). Nonlinear predictive optimization for deploying space tethered satellite via discrete-time fractional-order sliding mode. *IEEE Transactions on Aerospace and Electronic Systems*, *58*(5), 4517–4526. https://doi.org/10.1109/taes.2022.3166061

Lian, Z., Dong, Y., Yin, L., & Wang, Y. (2022). An economic evaluation method for LEO satellite constellation considering revenue and efficiency. In *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 488–493. https://doi.org/10.1109/ICCCWorkshops55477.2022.9896712

Liang, J., Chaudhry, A. U., & Yanikomeroglu, H. (2021). Phasing parameter analysis for satellite collision avoidance in Starlink and Kuiper constellations. In *2021 IEEE 4th 5G World Forum (5GWF)*, 493–498. https://doi.org/10.1109/5GWF52925.2021.00093

Lo, F.-Y., Rey-Martí, A., & Botella-Carrubi, D. (2020). Research methods in business: Quantitative and qualitative comparative analysis. *Journal of Business Research*, *115*, 221–224. https://doi.org/10.1016/j.jbusres.2020.05.003

Lobo, M. A., Moeyaert, M., Baraldi Cunha, A., & Babik, I. (2017). Single-case design, analysis, and quality assessment for intervention research. *Journal of Neurologic*

Physical Therapy: JNPT, *41*(3), 187–197. https://doi.org/10.1097/NPT.0000000000000187

Lohani, S., & Joshi, R. (2020, February). Satellite network security. In *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICONC345789.2020.9117553

Lucas, M. P., Dygert, N., Ren, J., Hesse, M. A., Miller, N. R., & McSween, H. Y. (2020). Evidence for early fragmentation-reassembly of ordinary chondrite (H, L, and LL) parent bodies from REE-in-two-pyroxene thermometry. *Geochimica et Cosmochimica Acta*, *290*, 366–390. https://doi.org/10.1016/j.gca.2020.09.010

Luu, M., & Hastings, D. E. (2021). Review of on-orbit servicing considerations for low-earth orbit constellations. ASCEND 2021, 4207. https://doi.org/10.2514/6.2021-4207

Magaldi, D., & Berler, M. (2020). Semi-structured interviews. *Encyclopedia of personality and individual differences*, 4825-4830. https://doi.org/10.1007/978-3-319-24612-3_857

Mahat-Shamir, M., Neimeyer, R. A., & Pitcho-Prelorentzos, S. (2021). Designing in-depth semi-structured interviews for revealing meaning reconstruction after loss. *Death Studies*, *45*(2), 83-90. https://doi.org/10.1080/07481187.2019.1617388

Mak, P. W., & Singleton, J. (2017). Burning questions: Exploring the impact of natural disasters on community pharmacies. *Research in Social and 157 Administrative Pharmacy, 13*(1), 162–171. https://doi.org/j.sapharm.2015.12.015

Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N. (2019). Detection of GPS spoofing attacks on unmanned aerial systems. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1–6. https://doi.org/10.1109/CCNC.2019.8651804

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

Marboe, I. (2019). Agreement on the rescue and return of astronauts and objects launched into outer space. In *Oxford research encyclopedia of planetary science*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190647926.013.65

Mark, C. P., & Kamath, S. (2019). Review of active space debris removal methods. *Space Policy*, *47*, 194–206. https://doi.org/10.1016/j.spacepol.2018.12.005

Martin, A. S., & Freeland, S. (2021). The advent of artificial intelligence in space activities: New legal challenges. *Space Policy*, *55*. https://doi.org/10.1016/j.spacepol.2020.101408

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*. https://doi.org/10.1177/2333393615597674

Megheirkouni, M., & Moir, J. (2023). Simple but effective criteria: rethinking excellent qualitative research. *The Qualitative Report*, *28*(3), 848-864. https://doi.org/10.46743/2160-3715/2023.5845

Melograna, C., & Johnson, C. (2024). Commercial space activities in the US: An overview of the current policy and regulatory framework. *Routledge Handbook of Commercial Space Law*, 42-64. https://doi.org/10.4324/9781003268475

Meng, Q., Liu, J., Zeng, Q., Feng, S., & Xu, R. (2019). Impact of one satellite outage on ARAIM depleted constellation configurations. *Chinese Journal of Aeronautics*, *32*(4), 967–977. https://doi.org/10.1016/j.cja.2019.01.004

Metcalfe, M. (2008). Pragmatic inquiry. *The Journal of the Operational Research Society*, *59*(8), 1091–1099. https://doi.org/10.1057/palgrave.jors.2602443

Migaud, M. R. (2020). Protecting earth's orbital environment: Policy tools for combating space debris. *Space Policy*, *52*, 1–9. https://doi.org/10.1016/j.spacepol.2020.101361

Millum, J., & Garnett, M. (2019). How payment for research participation can be coercive. *The American Journal of Bioethics*, *19*(9), 21-31. https://doi.org/10.1080/15265161.2019.1630497.

Mirick, R., & Wladkowski, S. (2019). Skype in qualitative interviews: Participant and researcher perspectives. *The Qualitative Report*, *24*(12), 3061–3072. https://doi.org/10.46743/2160-3715/2019.3632

Mitrea, T., Vasile, V., Borda, M., Nafornita, C., & Romaniuc, A. (2020). Study of attacks on satellite navigation system receivers. In *2020 13th International Conference on*

Communications (COMM), 521–525. https://doi.org/10.1109/COMM48946.2020.9141998

Mohan, A. S., & Kishore, A. (2021). Interactive multiple model approach to actuator fault detection, estimation and reconfiguration of a satellite launch vehicle. In *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, (pp. 1099–1104). https://doi.org/10.1109/ICECA52323.2021.9676096

Mohanty, S. (2021). Could future COP talks help to de-junk near-earth space? *Soundings*, *78*, 81–85. https://doi.org/10.3898/soun.78.05.2021

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Morin, J.-F., & Richard, B. (2021). Astro-environmentalism: Towards a polycentric governance of space debris. *Global Policy*, *12*(4), 568–573. https://doi.org/10.1111/1758-5899.12950

Motulsky, S. L. (2021). Is member checking the gold standard of quality in qualitative research?. *Qualitative Psychology*, *8*(3), 389. https://psycnet.apa.org/doi/10.1037/qup0000215

Mrusek, B., & Weiland, L. (2023, March). Space Commercialization and the Rise of Constellations: The Resulting Impact on the Kessler Effect. In *2023 IEEE Aerospace Conference* (pp. 01-07). IEEE. https://doi.org/10.1109/AERO55745.2023.10115734

Mullick, S., Srinivasa, Y., Sahu, A. K., & Sata, J. T. (2019). A comprehensive study on space debris, threats posed by space debris, and removal techniques. *SSRN Electronic Journal*, (pp. 876–883). https://doi.org/10.2139/ssrn.3511445

Muñoz-Patchen, C. (2018). Regulating the space commons: Treating space debris as abandoned property in violation of the Outer Space Treaty. *Chicago Journal of International Law*, *19*(1), 233–259. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1741&context=cjil

Mweshi, G. K., & Sakyi, K. (2020). Application of sampling methods for the research design. *Archives of Business Review*, *8*(11). https://doi.org/10.14738/abr.811.9042

Mwita, K. (2022). Factors influencing data saturation in qualitative studies. *International Journal of Research in Business and Social Science*, *11*(4), 414-420. https://doi.org/10.20525/ijrbs.v11i4.1776

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Nair, S. S., & Prem, S. S. (2020). A framework for mixed-method research. *Shanlax International Journal of Management*, *8*(2), 45–53. https://doi.org/10.34293/management.v8i2.3220

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education*, *8*(2), 90–97. https://doi.org/10.1007/s40037-019-0509-2

Nguyen, L., & Sparks, J. (2020). Air, space, and cyberspace: Reinvigorating defence of US critical infrastructure. *Air & Space Power Journal*, *34*(3), 44–53. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/V-Nguyen_Sparks.pdf

Ningi, A. I. (2022). Data Presentation in Qualitative Research: The Outcomes of the Pattern of Ideas with the Raw Data. *International Journal of Qualitative Research*, *1*(3), 196-200. https://doi.org/10.47540/ijqr.v1i3.448

Niyonsaba, S., Konate, K., & Soidridine, M. M. (2023). A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications*, *10*(5), 688-701. https://www.ijcna.org/Manuscripts/IJCNA-2023-O-46.pdf

Nudelman, M., & Orwig, J. (2015, October 9). History's best-known science satellites have evolved to enormous proportions. *Business Insider*. https://www.businessinsider.com/size-of-most-famous-satellites-2015-10

Office for Human Research Protections. (2021, March 10). *45 CFR 46*. U.S. Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html

Oldland, E., Botti, M., Hutchinson, A. M., & Redley, B. (2020). A framework of nurses' responsibilities for quality healthcare—Exploration of content validity. *Collegian*, *27*(2), 150-163. https://doi.org/10.1016/j.colegn.2019.07.007

Oliffe, J. L., Kelly, M. T., Gonzalez Montaner, G., & Yu Ko, W. F. (2021). Zoom interviews: Benefits and concessions. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211053522

Olivieri, L., & Francesconi, A. (2020). Large constellations assessment and optimization in LEO space debris environment. *Advances in Space Research: The Official Journal of the Committee on Space Research (COSPAR)*, *65*(1), 351–363. https://doi.org/10.1016/j.asr.2019.09.048

Pathiranage, Y. L., Jayatilake, L. V., & Abeysekera, R. (2020). Case study research design for exploration of organizational culture towards corporate performance. *Review of International Comparative Management/Revista de Management Comparat International*, *21*(3), 361-372. http://dx.doi.org/10.24818/RMCI.2020.3.361

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *HSR: Heakh Services Research*, *34*(5), 1189–1208.

Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac008

Phillips-Pula, L., Strunk, J., & Pickler, R. H. (2011). Understanding phenomenological approaches to data analysis. *Journal of Pediatric Health Care*, *25*(1), 67-71. https://doi.org/10.1016/j.pedhc.2010.09.004

Pirzada, S. J. H., Murtaza, A., Xu, T., & Jianwei, L. (2020). Architectural optimization of parallel authenticated encryption algorithm for satellite application. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2978665

Plano Clark, V. L. (2017). Mixed methods research. *The Journal of Positive Psychology*, *12*(3), 305–306. https://doi.org/10.1080/17439760.2016.1262619

Plotnek, J. J. (2022). A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems.

Pritchard, I. A. (2021). Framework for the ethical conduct of research: The ethical principles of the Belmont Report. In *Handbook of research ethics in psychological science* (pp. 3–21). American Psychological Association. https://doi.org/10.1037/0000258-001

Qasaimeh, M., Al-Qassas, R. S., & Ababneh, M. (2021). Software design and experimental evaluation of a reduced AES for IOT applications. *Future Internet*, *13*(11), 273. https://doi.org/10.3390/fi13110273

Rabjerg, J. W., Leyva-Mayorga, I., Soret, B., & Popovski, P. (2021). Exploiting topology awareness for routing in LEO satellite constellations. In *2021 IEEE Global Communications Conference (GLOBECOM)*, 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685686

Raguraman, S., Sarath, R. N. S., & Varghese, J. (2020). Space debris removal: Challenges and techniques-A review. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future*

Directions) (ICRITO), 1361–1366. https://doi.org/10.1109/ICRITO48877.2020.9197877

Ramsey, A., & Ramsey, J. (2019). Space Force and the Outer Space Treaty: One Small Step Forward for a Man, One Giant Leap Backward for Humankind. *USFL Rev. F.*, *54*, 4. https://bpb-us-w2.wpmucdn.com/usfblogs.usfca.edu/dist/7/272/files/2020/03/54-Forum_Ramsey.pdf

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care Part II: Data collection, analysis and results reporting. *Academic Emergency Medicine: Official Journal of the Society for Academic Emergency Medicine*, *22*(9), 1103–1112. https://doi.org/10.1111/acem.12735

Ratnapalan, S. (2019). Qualitative approaches: Variations of Grounded Theory Methodology. *Canadian Family Physician Medecin de Famille Canadien*, *65*(9), 667–668.

Rawnsley, A., & Hughes, S. (2019, October 22). Iranian hacking group targeted satellite industry nerds. *The Daily Beast*. https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies

Redd, N. T. (2020). Bringing satellites back from the dead: Mission extension vehicles give defunct spacecraft a new lease on life-[News]. *IEEE Spectrum*, *57*(8), 6-7. https://doi.org/10.1109/MSPEC.2020.9150540

Ren, S., Yang, X., Wang, R., Liu, S., & Sun, X. (2021). The Interaction between the LEO Satellite Constellation and the Space Debris Environment. *Applied Sciences*, *11*(20), 9490. https://doi.org/10.3390/app11209490

Riebeek, H., & Simmon, R. (2009). Catalog of Earth satellite orbits. *NASA Earth Observatory*. https://earthobservatory.nasa.gov/features/OrbitsCatalog

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8). https://doi.org/10.3390/s23084060

Rogers, D. (2022). *Broadband quantum cryptography*. Springer Nature. https://doi.org/10.1007/978-3-031-02513-6_1

Rome, J., Obenchain, M., Hartney, C., Chen, K., Villegas, A., Goyal, V. K., & Strizzi, J. (2023). Developing a roadmap for an on-orbit satellite factory concept. *AIAA SCITECH 2023 Forum*, 2687. https://doi.org/10.2514/6.2023-2687

Runnels, M. B. (2023). On Launching Environmental Law into Orbit in the Age of Satellite Constellations. *Journal of Air Law and Commerce*, *88*(1), 181. https://doi.org/10.25172/jalc.88.1.5

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR Journal of Research & Method in Education*, *12*(1), 22-29. https://doi.org/10.9790/7388-1201052229

Saad, A. I., Saad, N. H., & Ezzat, M. (2019). Combined power and attitude control system for low earth orbit satellites. In *2019 21st International Middle East*

Power Systems Conference (MEPCON), 447–452. https://doi.org/10.1109/MEPCON47431.2019.9008176

Sacchi, C., Granelli, F., Marchese, M., Cheung, K.-M., & Noble, M. (2022). Foreword to the special section on information and communication technologies (ICT) for a new space vision. *IEEE Transactions on Aerospace and Electronic Systems*, *58*(5), 3743–3745. https://doi.org/10.1109/taes.2022.3209856

Samanth, S., & Balachandra, M. (2022). Security in internet of drones: a comprehensive review. *Cogent Engineering*, *9*(1). https://doi.org/10.1080/23311916.2022.2029080

Sankaran, J. (2022). Russia's anti-satellite weapons: A hedging and offsetting strategy to deter Western aerospace forces. *Contemporary Security Policy*, *43*(3), 436–463. https://doi.org/10.1080/13523260.2022.2090070

Saqlain, M., Yu, X., Idrees, N. M., & Wang, S. (2021). Channel modeling and performance analysis of fixed terahertz Earth-satellite links in the low- and mid-latitude regions. *Optical Engineering*, *60*(3), 1–16. https://doi.org/10.1117/1.oe.60.3.036103

Savin-Baden, M., & Major, C. H. (2023). *Qualitative research: The essential guide to theory and practice*. Taylor & Francis.

Schafer, K., Horch, C., Busch, S., & Schafer, F. (2021). A Heterogenous, reliable onboard processing system for small satellites. In *2021 IEEE International Symposium on Systems Engineering (ISSE)*, 1–3. https://doi.org/10.1109/ISSE51541.2021.9582474

Schaus, V., Letizia, F., Virgili, B. B., & Lemmens, S. (2021). Leveraging space debris simulation results: Revisiting guideline values for explosion and cumulative collision rate. *8th European Conference on Space Debris, ESA/ESOC*. https://conference.sdo.esoc.esa.int/proceedings/sdc8/paper/162/SDC8-paper162.pdf

Secretary of the Air Force Public Affairs. (2020, May 13). *Satellite hacking challenge shifts to fully virtual event.* U.S. Air Force. https://www.af.mil/News/Article-Display/Article/2185826/satellite-hacking-challenge-shifts-to-fully-virtual-event/

Seeber, M. (2020). Framework and operationalisation challenges for quantitative comparative research in higher education. *Higher Education Quarterly*, *74*(2), 162–175. https://doi.org/10.1111/hequ.12245

Shaker, M. N., Tawakol, N. S., Amer, H. H., Daoud, R. M., & Adly, I. (2021). Dependability of electronic systems in the International Space Station. In *2021 16th International Conference on Computer Engineering and Systems (ICCES)*, 1–5. https://doi.org/10.1109/ICCES54031.2021.9686127

Shinn, M. (2022, September 23). In major step, space force takes over all military satellite communications. *The Gazette*. https://gazette.com/military/in-major-step-space-force-takes-over-all-military-satellite-communications/article_28ca61bc-3b51-11ed-bc6a-2752184fd423.html

Silva, M. E., Fritz, M. M., & El-Garaihy, W. H. (2022). Practice theories and supply chain sustainability: A systematic literature review and a research

agenda. *Modern Supply Chain Research and Applications*. https://doi.org/10.1108/MSCRA-01-2021-0001

Sim, J., & Waterfield, J. (2019). Focus group methodology: Some ethical challenges. *Quality & Quantity*, *53*(6), 3003-3022. https://doi.org/10.1007/s11135-019-00914-5

Simon, R. (2016). The conflict paradigm in sociology and the study of social inequality: Paradox and possibility. *Theory in Action*, *9*(1), 1–31. https://doi.org/10.3798/tia.1937-0237.16001

Singh, N., Benmamoun, M., Meyr, E., & Arikan, R. H. (2021). Verifying rigor: Analyzing qualitative research in international marketing. *International Marketing Review*, *38*(6), 1289-1307. https://doi.org/10.1108/IMR-03-2020-0040

Singh, S., & Purbey, S. (2022). Space debris – it's effect on the earth. *International Journal of Recent Advances in Multidisciplinary Topics*, *3*(6), 13–16. https://journals.resaim.com/ijramt/article/view/2135

Sladen, R. (2020). *Iridium constellation status*. http://www.rod.sladen.org.uk/iridium.htm

Sorce, G. (2019). Institutional ethnography for communication and media research. *The Communication Review*, *22*(4), 296–308. https://doi.org/10.1080/10714421.2019.1659703

Sowell, S., & Taheri, E. (2022). Minimum-time and minimum-fuel low-thrust trajectory design for satellite formation in low-earth orbits. In *2022 American Control Conference (ACC)*, 2938–2943. https://doi.org/10.23919/ACC53348.2022.9867708

Stahl, N. A., & King, J. R. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education*, *44*(1), 26-28.

Stein, V., Wiedemann, A., & Bouten, C. (2019). Framing risk governance. *Management Research Review*, *42*(11), 1224-1242. https://doi.org/10.1108/MRR-01-2019-0042

Stone, A. A., Schneider, S., & Smyth, J. M. (2023). Evaluation of pressing issues in ecological momentary assessment. *Annual Review of Clinical Psychology*, *19*, 107-131. https://doi.org/10.1146/annurev-clinpsy-080921-083128.

Surdi, S. A. (2020). Space Situational Awareness through Blockchain Technology. *The Journal of Space Safety Engineering*, *7*(3), 295–301. https://doi.org/10.1016/j.jsse.2020.08.004

Sürücü, L., & Maslakci, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694-2726. https://doi.org/10.15295/bmij.v8i3.1540

Taherdoost, H. (2022). What are different research approaches? Comprehensive Review of Qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, *5*(1), 53-63. https://doi.org/10.30564/jmser.v5i1.4538

Tan, Z., Qin, H., Cong, L., & Zhao, C. (2019). New method for positioning using IRIDIUM satellite signals of opportunity. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 83412–83423. https://doi.org/10.1109/access.2019.2924470

Tashakkori, A., Johnson, R. B., & Teddlie, C. (2020). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Sage Publications, Inc.

Thayer, J. P., Tobiska, W. K., Pilinski, M. D., & Sutton, E. K. (2021). Remaining issues in upper atmosphere satellite drag. *Space weather effects and applications*, 111-140. https://doi.org/10.1002/9781119815570.ch5

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing-Quarterly Scientific*, 155–163. https://doi.org/10.5281/ZENODO.2552022

Tian, M., Chen, Y., Tian, G., Huang, W., & Hu, C. (2023). The role of digital transformation practices in the operations improvement in manufacturing firms: A practice-based view. *International Journal of Production Economics*, *262*. https://doi.org/10.1016/j.ijpe.2023.108929

Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science*, *3*, 881-887. https://doi.org/10.1016/j.procs.2010.12.144

Tomizaki, H., Kobayashi, R., Suzuki, M., Karasawa, N., Hasegawa, S., & Makihara, K. (2021). Assessment of space debris collisions against spacecraft with deorbit devices. *Advances in Space Research: The Official Journal of the Committee on Space Research*, *67*(5), 1526–1534. https://doi.org/10.1016/j.asr.2020.12.018

Torky, M., Hassanein, A. E., El Fiky, A. H., & Alsbou, Y. (2019). Analyzing space debris flux and predicting satellites collision probability in LEO orbits based on

Petri nets. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 83461–83473. https://doi.org/10.1109/access.2019.2922835

Trevino, M. B. (2021). *Space race*. Salem Press Encyclopedia.

Trishchenko, A. P., Garand, L., & Trichtchenko, L. D. (2019). Observing polar regions from space: Comparison between highly elliptical orbit and medium Earth orbit constellations. *Journal of Atmospheric and Oceanic Technology*, *36*(8), 1605–1621. https://doi.org/10.1175/jtech-d-19-0030.1

Tu, Z., Zhou, H., Li, K., Li, M., & Tian, A. (2020). An energy-efficient topology design and DDoS attacks mitigation for green software-defined satellite network. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 211434–211450. https://doi.org/10.1109/access.2020.3039975

U.S. Space Force. (2022). *Personnel doctrine for space forces*. Space Doctrine Publication. https://www.starcom.spaceforce.mil/Portals/2/SDP%201-0%20Personnel%207%20September%202022.pdf?ver=erudfM8rwArAPlxplIu47g%3d%3d%201-0%20Personnel%207%20September%202022.pdf%20(spaceforce.mil)

Van Camp, C., & Peeters, W. (2022). A world without satellite data as a result of a global cyber-attack. *Space Policy*, *59*. https://doi.org/10.1016/j.spacepol.2021.101458

Varadarajan, R. (2020). Customer information resources advantage, marketing strategy, and business performance: A market resources-based view. *Industrial Marketing Management*, *89*, 89-97. https://doi.org/10.1016/j.indmarman.2020.03.003

Varadharajan, V., & Suri, N. (2023). Security challenges when space merges with cyberspace. *Space Policy.* https://doi.org/10.1016/j.spacepol.2023.101600

Vićić, J., & Harknett, R. (2024). Identification-imitation-amplification: Understanding divisive influence campaigns through cyberspace. *Intelligence and National Security*, 1-18. https://doi.org/10.1080/02684527.2023.2300933

Walker, R. (2019). *Potential severe effects of a biosphere collision and planetary protection implications* (pp. 1–131). https://doi.org/10.31219/osf.io/kad38

Wall, J. (2017, February 8). *What is a satellite?* NASA. https://www.nasa.gov/audience/forstudents/k-4/stories/nasa-knows/what-is-a-satellite-k4.html

Wang, C., & Song, Z. (2019). Trajectory optimization for reusable rocket landing. *2019 Chinese Automation Congress (CAC)*, 3052–3057. https://doi.org/10.1109/CAC48633.2019.8997476

Wang, D., Liu, Z., Zhou, J., Yang, J., Chen, X., Chang, C., & Hu, J. (2022). Barriers to implementation of enhanced recovery after surgery (ERAS) by a multidisciplinary team in China: A multicenter qualitative study. *BMJ Open*, *12*(3). http://dx.doi.org/10.1136/bmjopen-2021-053687

Wang, F., Zhang, C., & Sun, H. (2019). Research on the space-time anti-jamming algorithm for satellite navigation receivers. In *2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, 617–621. https://doi.org/10.1109/ICISCAE48440.2019.221708

Wang, R., Liu, W., Yan, R., Shi, L., & Liu, S. (2020). Refined study of space debris collision warning techniques for LEO satellites. *The Journal of Space Safety Engineering*, *7*(3), 262–267. https://doi.org/10.1016/j.jsse.2020.07.018

Wiles, R., Crow, G., Heath, S., & Charles, V. (2008). The management of confidentiality and anonymity in social research. *International Journal of Social Research Methodology*, *11*(5), 417-428. https://doi.org/10.1080/13645570701622231

Winwood, J. (2019). Using interviews. In *Practical research methods in education* (pp. 12-22). Routledge.

Wutich, A., & Brewis, A. (2019). Data collection in cross-cultural ethnographic research. *Field Methods*, *31*(2), 181–189. https://doi.org/10.1177/1525822x19837397

Xie, Y., Chan, K., & Zhang, J. (2020). Collision probability of composite cubesats hovering in leader-follower configuration. *Acta Astronautica*, *168*, 211–219. https://doi.org/10.1016/j.actaastro.2019.12.011

Yang, X. (2020). *Low earth orbit (LEO) mega constellations - Satellite and terrestrial integrated communication networks* [Doctoral dissertation, University of Surrey]. https://doi.org/10.15126/THESIS.00850382

Yue, P., An, J., Zhang, J., Pan, G., Wang, S., Xiao, P., & Hanzo, L. (2022). On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends. *arXiv preprint.* https://doi.org/10.48550/arXiv.2201.03063

Yue, P., An, J., Zhang, J., Ye, J., Pan, G., Wang, S., ... & Hanzo, L. (2023). Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.48550/arXiv.2201.03063.

Zander, M. E., Chamberlain, M. K., Jost, D., Müller, D. R., Hagmeister, N., Straubel, M., & Hühne, C. (2023). Design and testing of the BionicWingSat in a zero-g flight campaign - A 2U-CubeSat with deployable, biologically-inspired wings. *AIAA SCITECH 2023 Forum*, 2697. https://doi.org/10.2514/6.2023-2697

Zhang, H., Wang, Y., & Song, M. (2019). Does competitive intensity moderate the relationships between sustainable capabilities and sustainable organizational performance in new ventures? *Sustainability*, *12*(1), 253. https://doi.org/10.3390/su12010253

Zhang, X., Xiao, K., & Gu, J. (2022). The development of radar and radar countermeasure. In *Theory to Countermeasures Against New Radars* (pp. 1–63). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-6715-2_1

Zhang, Y., Wang, Y., Hu, Y., Lin, Z., Zhai, Y., Wang, L., Zhao, Q., Wen, K., & Kang, L. (2022). Security performance analysis of LEO satellite constellation networks under DDoS attack. *Sensors, 22*(19), 1–10. https://doi.org/10.3390/s22197286

Zhao, Y., Zhang, F., & Huang, P. (2022). Dynamic closing point determination for space debris capturing via tethered space net robot. *IEEE Transactions on Aerospace and Electronic Systems*, *58*(5), 4251–4260. https://doi.org/10.1109/taes.2022.3159626

Zhou, Y., Liu, J., Zhang, R., Liu, F., Huang, T., & Chen, T. (2022). A congestion-aware handover scheme for LEO satellite networks. In *2022 IEEE/CIC International Conference on Communications in China (ICCC)*, 896–901. https://doi.org/10.1109/ICCC55456.2022.9880720

Zhu, P., Tang, X., Wu, D., Goli, M., & Fang, W. (2022). The total solar irradiance as measured from space since 1978. *Authorea Preprints*. https://doi.org/10.1002/essoar.10509885.1

Zhu, W., Pang, Z., Si, J., & Gao, G. (2022). Dynamics and configuration control of the Tethered Space Net Robot under a collision with high-speed debris. *Advances in Space Research: The Official Journal of the Committee on Space Research*, *70*(5), 1351–1361. https://doi.org/10.1016/j.asr.2022.06.019

Zyphur, M. J., & Pierides, D. C. (2017). Is quantitative research ethical? Tools for ethically practicing, evaluating, and using quantitative research. *Journal of Business Ethics*, *143*(1), 1–16. https://doi.org/10.1007/s10551-017-3549-8

Appendix A: Collaborative Institutional Training Initiative Certification

CITI PROGRAM

Completion Date 17-Jan-2021
Expiration Date N/A
Record ID 40409139

This is to certify that:

Nathaniel Juarez

Not valid for renewal of certification through CME.

Has completed the following CITI Program course:

Student's
(Curriculum Group)
Doctoral Student Researchers
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

101 NE 3rd Avenue, Suite 320
Fort Lauderdale, FL 33301 US
www.citiprogram.org

Appendix B: Interview protocol

1. Document interview location, time (in Eastern Standard Time (EST)), date and name of the participant.
2. Provide participant with my introduction as the researcher.
3. Explain that participation from the participant is strictly voluntary and they can choose to end/cancel the interview at any time.
4. Inform the participants that their interview answer will be confidential, and their identities or company of employment will not be disclosed in any part of the publication created from this study.
5. Describe the purpose of the study is to identify strategies used to rapidly decommission IT satellites from LEO that are vulnerable to cyber-attacks without adding to Kessler Syndrome phenomenon.
6. Describe the overall benefits of the study and how the results may be used to improve strategies to decommission IT satellites from LEO that are vulnerable to cyber-attacks without adding to Kessler Syndrome phenomenon.
7. Ensure the interviewee is comfortable and feels like they are in a safe environment to speak.
8. Inform the participant that the interview is starting and recording will be utilized and kept for five years before being destroyed. Reassure the participant that the information will be encrypted, and password protected on both the primary and back-up hard drives.

9. As the semi-structed interview questions and bring up any follow up questions needed for clarification.
10. Inform the participant that the interview is concluding and document the time if the participant does not have any follow-up questions or go backs.
11. Inform the participant that transcription software will be used to transcribe our conversation to text.
12. Send the converted text to the interviewee to confirm that transcription accurately captures their viewpoints and is free of errors.
13. Give thanks to the interviewee/participant for taking time to aid in the study.