THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

Space Worms: On the Threat of Cyber-ASAT Weaponry to Satellite Constellations

RAJIV THUMMALA
SPRING 2023

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Cybersecurity Analytics and Operations
with honors in Cybersecurity Analytics and Operations

Reviewed and approved* by the following:

Peng Liu
Raymond G. Tronzo, MD Professor of Cybersecurity
Thesis Supervisor

Michael Hills
Teaching Professor of Information Sciences and Technology
Honors Adviser

* Electronic approvals are on file.

ABSTRACT

Surging contentions between adversarial nation-states over the space domain has induced the global proliferation of anti-satellite (ASAT) weapons. However, international concerns over collateral space debris and the eventuation of the Kessler Syndrome has caused the public retraction of such armaments. It is consequently expected that the next generation of space warfare will feature cyber-ASAT weapons which bear the capability to breach a satellite without the ramification of debris. Amongst the array of potential space-based targets, satellite constellations are especially vulnerable to cyber-ASAT weapons due to their inter-agent nature and expansive attack surface. While there have been no publicly reported instances of a satellite-to-satellite cyberattack, it is affirmed that this threat is not merely theoretical. By emulating the deployment of a cyber-ASAT weapon against an operational satellite constellation, this thesis demonstrates the capability for a malicious actor to exploit satellite-to-satellite crosslinks to cause damage. Subsequently, the danger of worm propagation throughout satellite constellations is highlighted.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to begin by thanking my parents for supporting my academic and professional endeavors.

I would also like to thank the NASA Pennsylvania Space Grant Consortium, Virtual Student Federal Service, and Oak Ridge Institute for Science and Education for setting me on the path to pursue my passion for securing the aerospace domain. I am indebted to the countless mentors and faculty members who went out of their way to guide me throughout my academic career.

I am especially thankful to the Schreyer Honors College for sparking my academic pursuits and providing me with all the resources to succeed.

Chapter 1
Introduction

1.1 Overview

Space is essential to the modern way of life, enabling assets that play critical roles in a myriad of critical infrastructures, systems, and operations. This includes but is not limited to power grids, financial transactions, global positioning systems (GPS), telecommunication services, weather forecasting, air travel, gas pumps, traffic lights, cell phones, surveillance, emergency response, and warfare. As echoed by the United States Space Force (USSF), there is no such thing as a day without space operations [1].

The accessibility to space has significantly evolved since the USSR's launch of *Sputnik* on October 4th, 1957, and the United States' launch of *Explorer 1* on January 31st, 1958. Initially constrained to first-world nation states and public sectors due to budgetary obligations and lack of commercial incentives, space has now become accessible to private companies, universities, and civilians across the globe. Commercial organizations such as SpaceX have significantly contributed to the American conquest of space, deploying upwards of 3,000 satellites, and accomplishing invaluable engineering feats such as the development of re-usable rockets. In recognition of the benefits that the commercial presence in space provides, relationships between the public and private sector have significantly developed over the past decade through mediums such as federal

contracts. This relationship is expected to bolster in the coming years as efforts persist to foster a robust public-private space ecosystem.

Increased accessibility to the space domain will inevitably escalate the dependence on space-based assets to enable critical infrastructure, systems, and operations. This factor is a driving force behind the militarization and global contest of space. Breaching critical space-based assets could have catastrophic consequences to a populace, resulting in significant economic setbacks and/or even death. Despite the criticality of the space sector, in the United States space has yet to be designated as a critical infrastructure. As a result, threats to the space sector have largely been overlooked and have only recently begun to receive attention from entities such as the Department of Homeland Security (DHS) [2]. Especially of concern are non-kinetic threats (i.e.: cyberattacks) to critical space-based assets due to the novelty of the threat and consequent lack of sufficient technical capabilities for defense. Offering unique benefits such as anonymity, repudiation, and cost-effectiveness, cyberspace serves as an optimal medium for adversaries to attack space systems. The threat of cyber-ASAT weapons against space systems only continues to grow as the accessibility to powerful radio equipment, malicious script kiddies, open-source offensive security tools, and SATCOM enabled technologies is becoming increasingly pervasive [3].

This study identifies, assesses, and examines the threat of cyberattacks to a specific classification of space technology: satellite constellations. Particular emphasis is placed on the distinctive consequences of worms deployed on inter-connected satellites in comparison to standalone space vehicles. In addition to evaluating existing literature, policy, and efforts to mitigate worm propagation in satellite constellations, the feasibility

to breach a space vehicle through the exploitation of crosslinks is demonstrated through emulation. Solutions are subsequently proposed to harden satellite constellations from cyber-ASAT weapons.

1.2 Problem Statement and Research Objectives

The advent of interconnectivity capabilities amongst space vehicles has revolutionized the value, efficiency, and effectiveness of space-based operations. However, akin to cyber-physical systems engineered to operate in terrestrial environments, space vehicles were not designed with cybersecurity in mind. While efforts have persisted in recent years to integrate cyber-defense mechanisms into critical space-based assets, these initiatives are still nascent. By extension, cyber-threats to niche space-based architectures and technologies (i.e.: satellite constellations, ISAM subsystems, orbital stations, space telescopes, etc.) have received little to no attention. Attributed to the agile maturation of offensive cyber capabilities in comparison to the deployment of novel cybersecurity mechanisms aboard space-based assets, if this trajectory persists, it is inevitable that these space-based architectures and technologies will be compromised by malicious actors.

With the intention to remediate this void of inquiry, this study explores the threat of cyber-ASAT weapons to satellite constellations. There are three fundamental objectives for this thesis and are enumerated as follows.

1. *Demonstrate the technical capability and potential impacts of employing cyber-ASAT weaponry to exploit vulnerabilities in satellite-to-satellite crosslinks*

The cybersecurity landscape frequently finds itself in a reactive state, as defensive measures are typically implemented only after a significant breach has occurred. This is not acceptable in the space domain as there is little wiggle room to update the security of an asset following deployment due to lack of physical access. While this assertion has been acknowledged to an extent in industry, it is outweighed by concerns of the viability of developing threats genuinely posing an affect to an asset. For instance, there has been extensive alarm over the threat of quantum-enabled cyberattacks towards satellites in recent years [4]. However, there have been no significant events nor viable demonstrations of such an attack. As a result, defending satellites against quantum-powered cyberattacks has not been a primary focus of R&D. Similarly, there exists literature regarding the plausibility of a space-to-space cyberattack, but no technical demonstrations of such an attack. By successfully demonstrating the technical capability and viability of a satellite-to-satellite cyberattack through emulation, I aim for this research to serve as a point of reference to refute claims that this threat is merely theoretical.

2. *Provide practical solutions for government and commercial entities to thwart the propagation of worms in satellite constellations.*

While emphasizing the criticality of this threat is a primary focus of this thesis, I also seek to point to the initial direction that should shape the next phase of R&D in this area. Proposing practical and feasible solutions as opposed to far-fetched engineering goals is of particular importance in taking a swift approach to resolving this issue.

3. *Raise awareness to the significance of cybersecurity threats against satellite constellations and the exigency to develop defenses.*

This thesis seeks to function as a call-to-action, raising awareness to the threat of worm propagation in satellite constellations and the necessity to conduct further R&D in this area. Ultimately, I aim for this thesis to prompt commercial vendors and government entities to take preemptive action before an inevitable attack occurs.

1.3 Space-Based Non-Kinetic Warfare

Fortunately, adversarial nation-state electromagnetic pulse attacks and cyberattacks on critical space systems have been infrequent. However, it is certain that the conspicuous increase in civilian and military dependence on these apparatuses will spotlight them as compelling attack vectors. Initially anticipating the dangers of non-kinetic warfare during the Cold War, the U.S. Army had a healthy concern for a defensive space-based electronic posture. For instance, the 1980s featured the advents of

null steering mechanisms such as The Steerable Null Antenna Processor (SNAP-1) and the Plessey Interference Cancellation System. Both of these architectures provided the ability to thwart undesirable interference and jamming. This concern has dwindled, however, following the decline of the Soviet Union which enabled the U.S. Army to relax its emphasis on the electronic warfare threat [5].

With cyber and electronic weaponry becoming pervasive amongst adversarial nations, it is no longer sufficient to sustain this apathy. Nations such as China and Russia have extensively leveraged cyber-warfare as a medium of attack due to its obfuscated and anonymous nature.

Non-kinetic warfare in particular is expected to serve as the primary medium of space-based attack in the coming decades, due to an anticipated ban on strike weapons in the Outer Space Treaty [6] [7]. In fact, the United States has already decided to implement a self-imposed ban on the testing of anti-satellites weapons, in part to highlight a Russian test in November that created a dangerous field of space debris [8]. Thus, we can conjecture that cyber-ASAT weaponry will play a key role in impending space-combat.

1.4 Overview of Satellite Systems

This section adumbrates the basic fundamentals of satellite systems needed to comprehend the content in the succeeding chapters.

1.4.1 Utility of Satellites

The application versatility of satellites has evolved significantly since the launch of Sputnik on October 4th, 1957. Originally developed to serve as a communication apparatus, satellites have at a fundamental level adhered to this mission. In the 21st century, satellites are essential to the modern way of life, playing critical roles in a multitude of critical infrastructures & safety critical systems (SCS) [3].

In comparison to terrestrial vehicles, satellite systems offer a unique array of benefits that make them attractive for niche operations. For instance, satellites enable entities to have global coverage, remediating any hinderances caused by geographic or political boundaries. This makes satellite systems optimal for navigation, observation, and communication. Satellites also provide a larger coverage or field of view (FOV) in comparison to terrestrial vehicles which are bound by physical restrictions. Namely, terrestrial vehicles are limited to a narrow line of sight which can only be altered by changing altitude or position. Satellites, on the other hand, are much more efficient in that they bolster the capability to cover extensive areas of interest with just a single pass.

The applications of satellite systems can be segmented into five primary components: communication, navigation, transportation, planetary observation, and military. In the domain of communication, satellites enable a wide range of services such

as radio, television, internet, and telephone. Entities in remote locations are especially dependent on satellites to enable these services due to the lack of terrestrial apparatuses and networks. Navigation systems are directly dependent on satellite systems such as the Global Navigation Satellite System (GNSS) to enable coverage. Systems such as GPS receivers function by receiving signals from multiple satellites within a constellation and perform calculations to provide users with accurate and reliable positioning, navigation, and timing (PNT) services. Transportation systems--especially aerial vehicles--are directly dependent on satellites to enable operations such as communication, navigation, and traffic management. Satellites are also often deployed for planetary observation and subsequent scientific research purposes. For instance, the National Oceanic and Atmospheric Administration (NOAA) operates the Geostationary Operational Environmental Satellite (GOES) constellation which provides critical data for hurricane forecasting and studies related to climate change [9]. The military employs satellites extensively for intelligence purposes and to serve as a robust method of communication. In contrast to other mediums of communication, satellites are of especial use in military applications as they are highly reliable and can be employed in remote areas such as the ocean.

1.4.2 Conventional Satellite Communication Architecture

The communication architecture for a satellite system is variable and is largely dependent on the specific use-case. However, most satellite system architectures can be abstracted into the following three segments: the space segment, user segment, and

ground segment. The space segment consists of the assets that are in orbit, including the space vehicle, antenna. and other in-situ components that enable communication with the ground segment. It is particularly responsible for relaying signals between ground stations. The user-segment refers to the endpoint equipment that is employed to access the services provided by the space segment. This includes but is not limited to satellite phones, GPS receivers, and satellite internet modems. The ground segment consists of the ground-based infrastructure that is utilized to communicate with the assets that compose the space segment. This segment therefore consists of ground stations or terminals that are utilized to transmit and receive signals to and from the satellites. Associated equipment utilized to process and/or route signals are also classified into the ground segment. A high-level abstraction of this conventional architecture is illustrated in figure 1.

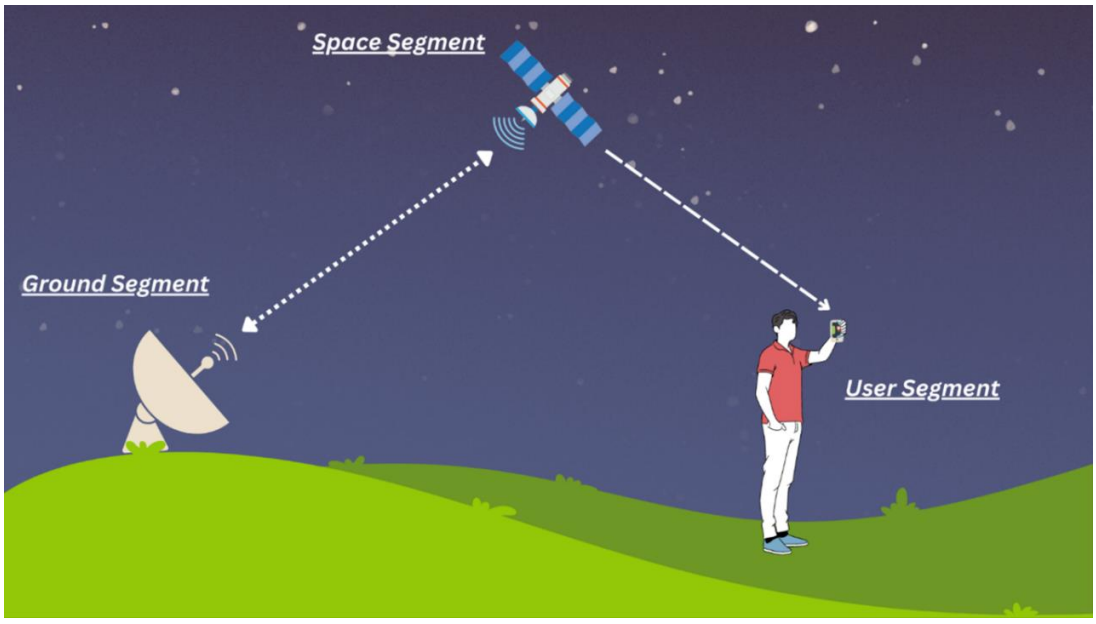

Figure 1. Conventional Satellite Communication Architecture

1.4.3 Major Satellite Subsystems and Components

Satellites are composed of a variety of subsystems and components that work in tandem to achieve mission objectives. While these subsystems can vary depending on the use-case, the major subsystems of a satellite include the command and data handling subsystem (CDHS), attitude determination and control subsystem (ADCS), thermal subsystem, propulsion subsystem, and the payload.

The CDHS functions as the brain of the satellite and is tasked with enabling the transmission and receiving of data between the ground station and the vehicle. It consists of a variety of components including modulation/demodulation systems, a solid state recorder, and space flight computer [10]. The power subsystem leverages components such as solar panels and batteries to provide electrical power to the satellite. The propulsion subsystem is responsible for controlling the satellite's movement and maintaining its position in orbit. It consists of components such as fuel tanks and thrusters. The ADCS is responsible for controlling both the orientation and stability of the satellite and includes components such as magnetometers and reaction wheels. The thermal control subsystem's primary purpose is to regulate the temperature of the satellite by leveraging components such as heaters, radiators, and insulation. The payload is unique to each satellite and carries the mission's scientific instruments and apparatuses necessary to achieve mission objectives.

These subsystems are by no means exhaustive. It is important to emphasize that satellites are heavily reliant on inter-process communications and require subsystems to

work in tandem to achieve mission objectives. Thus, in some instances subsystems may be conjoined.

1.5 Integration of Satellites in Critical Infrastructure

As aforementioned, satellites have increasingly integrated with critical infrastructure over the past decades. In fact, satellites play an intermediary role in nearly all of the 16 critical infrastructure sectors as designated by CISA. Sectors that make extensive use of satellite systems are highlighted as follows.

1.5.1 Chemical Sector

Satellites serve as a key technology to monitor chemical facilities for potential signatures and/or hazardous events. They provide an early warning to authorities in addition to enabling swift incident response. While chemical facilities do not solely depend on satellites to perform this monitoring operation, they significantly assist in obtaining data that can be utilized to pinpoint the origin of a potential leak [11].

1.5.2 Commercial Facilities Sector

In the commercial facilities sector, satellites are employed to assist in real-time monitoring efforts. As previously mentioned, satellites serve as optimal technologies to assist in surveillance of a large area that cannot be accomplished by traditional cameras.

These monitoring efforts can be utilized to warn respective respondents about potential threats that should be addressed, ultimately preventing adverse events.

1.5.3 Communications Sector

Satellites are integral to a variety of communication apparatuses across civilian and military domains. They are primarily tasked with enabling critical infrastructure for communication apparatuses including but not limited to cellular networks, satellite phones, GPS systems, and television. In comparison to the preceding sectors, the communication sector is directly dependent on the availability of satellites to perform its functions.

1.5.4 Defense Industrial Base Sector

Satellites are extensively employed in military and defense contexts for surveillance and communication purposes. In addition to being concealed from the general public, satellites are more reliable and offer benefits such as global coverage. This provides extensive utility in intelligence gathering as well as emergency response.

1.5.5 Financial Services Sector

The functionality and security of financial transactions are often directly dependent on satellites. Satellites are employed to monitor financial transactions (data streams) in addition to facilitating the identification of fraud. Furthermore, satellites are a

primary enabler for cross-border banking transactions. Akin to the commercial facilities sector, satellites are also utilized to monitor the physical security of financial institutions and subsequently assist in incident response.

1.5.6 Nuclear Reactors, Materials, and Waste Sector

Nuclear facilities are often monitored by satellites through payloads equipped with thermal imaging and radioactive emission sensors [12]. These capabilities ensure a safe and secure nuclear environment by warning incident response specialists of potential dangers. Furthermore, they facilitate the secure transportation and disposal of nuclear waste.

1.5.7 Food and Agriculture Sector

The food and agriculture sector extensively depends on satellites to assist in monitoring and assisting in analyzing vegetation, crop yields, weather patterns, other factors that play a role in breeding agriculture [13]. This ensures that the production of food is both safe and efficient. Furthermore, this gleaned data assists in scientific research endeavors that aim to optimize the agriculture sector.

1.5.8 Transportation Sector

As aforementioned, transportation systems in the modern day extensively rely on satellites to enable operations such as navigation and air traffic control. This dependency

is expected to increase as more transportation systems remediate their air-gapped architecture in place of IoT devices that rely on satellites. The utility of satellites in transportation is expansive and includes but is not limited to ATC, GPS navigation, monitoring of transportation infrastructure, and tracking of marine vessels.

1.5.9 Reflection

This synopsis is by no means exhaustive, as satellites play a role either directly or indirectly in nearly all the 16 critical infrastructure sectors designated by CISA. It must also be noted that a myriad of critical infrastructures are directly dependent on the availability of satellites. For these infrastructures, satellites act as a single-point-of-failure (SPOF) in the sense that their failure will cause cascading effects to reliant entities. Excluding systems that are equipped with sufficient redundancy measures, an intentional breach of a satellite will indubitably disable these dependent infrastructures. It is therefore paramount that extensive resources are allocated to researching and deploying robust mechanisms capable of securing satellites from the full gamut of threats.

1.6 Overview of Satellite Constellations

Satellite constellations, also referred to as interconnected satellites, are a network of space vehicles that are intentionally placed into orbit in a specific pattern or configuration. Operating as a proliferated architecture, this system provides a wide array of benefits in comparison to standalone conventional satellites. They are specifically

designed to function in cohesion to optimize services such as navigation, communications, remote sensing, and scientific research. This section will adumbrate the fundamentals of satellite constellations needed to comprehend the succeeding chapters.

1.6.1 History of Satellite Constellations

The first commercial satellite constellations were developed by Iridium and Globalstar. Iridium launched a constellation consisting of 66 satellites into LEO for global communication services, while Globalstar launched a constellation of 48 satellites for phone and data services. Iridium's first constellation is now a legacy fleet and has largely been deorbited in place of a new constellation--'Iridium Next' [14].

Between 2002 and 2003, the concept of utilizing satellite constellations for earth observation was first introduced with the launch of satellites for the Disaster Monitoring Constellation (DMC). The DMC consisted of five satellites in total and assisted in rapid response capabilities for natural disasters and other emergencies [15]. It was utilized for monitoring the effects and aftermath of the Indian Ocean Tsunami which occurred in December of 2004 as well as after Hurricane Katrina which occurred in August of 2005 [15].

In the 2010s, advancements in technology and increasing demands for global communication services led to the development of larger satellite constellations. Specifically, SpaceX launched their plans of delivering thousands of satellites into LEO for providing internet coverage [16]. OneWeb also revealed their intention to launch a mega-constellation of 650 satellites [20]. Other constellations such as the Telesat LEO

constellation [17] and Amazon Kuiper [18] constellation were also announced to the public.

Starlink—the most well-known satellite constellation (pictured in figure 2)—is operated by SpaceX and features over 3,580 satellites in LEO as of February 2023 [19]. This constellation seeks to provide internet to those in remote regions who do not have access to robust network environments. The first fleet of Starlink satellites was only launched in 2019 and has amassed more than 1 million subscribers as of January of 2023. SpaceX is expected to launch 12,000 more satellites in the coming years with a possible later extension to 42,000 [21].

Figure 2. Fleet of Starlink Constellations as viewed from Earth [23]

As previously mentioned, commercial entities such as SpaceX have already deployed constellations consisting of thousands of satellites in the span of less than 5

years. It is certain that this frequency of deployments will only escalate in the coming years across the space sector, as launching assets into orbit becomes more affordable and feasible. This emphasizes the significance and momentous nature of the impending threat discussed in this work.

1.6.2 Utility of Satellite Constellations

There is an array of benefits that satellite constellations offer over conventional standalone satellites. One major benefit is increased coverage, as constellations provide a significant increase in field of view in contrast to standalone satellites that can only cover a limited area at a given time. This is useful for instances that require time-sensitive data as constellations require less passes to glean data from a target. One example is the previously discussed DMC Constellations which assisted in providing real-time data regarding Hurricane Katrina. Constellations also tend to bolster more redundancy over conventional satellite systems in that the mission can still be accomplished if a singular satellite within the fleet fails. Furthermore, the proliferated nature of satellite constellations enables lower latency due to the ability to implement advanced network architectures and access techniques. This makes constellations a great utility for internet applications such Starlink. Constellations are also known to be more flexible in contrast to their conventional standalone satellite counterparts. Namely, constellations can be configured to allow for changes in coverage, capacity, and mission objectives. This is especially important in dynamic environments such as Earth observation or disaster response where changes may need to be made following deployment. Overall, satellite

constellations offer immense utility for a wide range of applications and will continue to grow in this regard.

1.6.3 Satellite Constellation Conventional Architecture

While the communication architecture for a satellite constellation will vary depending on the mission objectives, all constellations will involve a combination of intersatellite (satellite-to-satellite) links (also referred to as “crosslinks”) and space-to-ground links. Satellites in a constellation operate as a relay network in which each satellite within the constellation functions as a node. Crosslinks enable the relay of data between satellites within the constellation and ground links enable communication with the ground station (see figure 3).

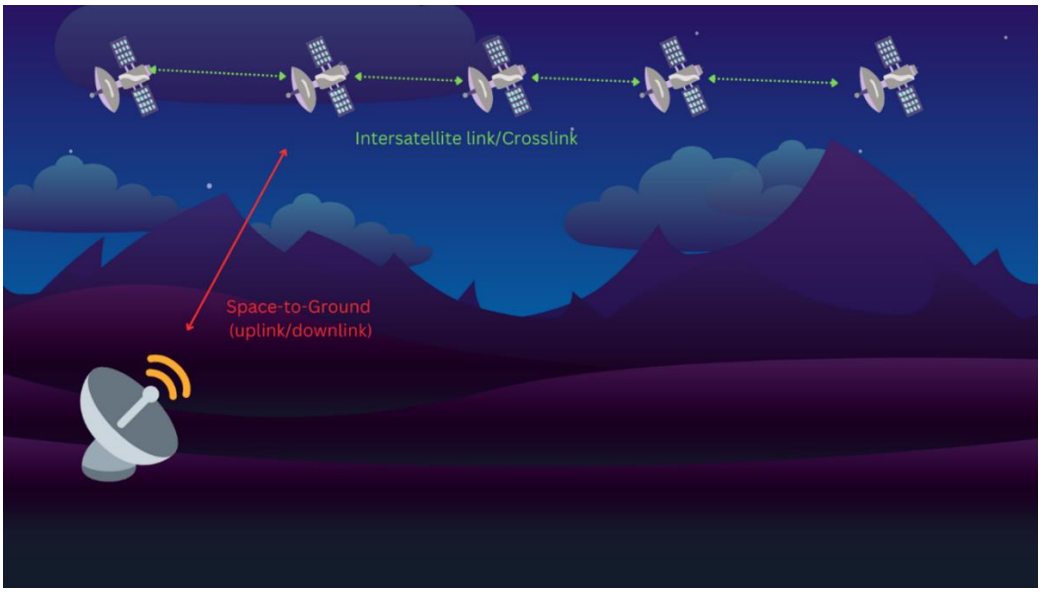

Figure 3. Fundamental Satellite Constellation Communication Architecture

Some constellations opt to utilize a mesh network architecture in which each satellite bears the capability to communicate with another satellite. However, others may utilize a centralized architecture in which each satellite within the constellation primarily communicates with a singular hub or gateway. This largely depends on the purpose of the mission and factors such as coverage, reliability, and latency. In general, crosslinks are utilized to relay commands between satellites, establish network topology, or support system level functions such as synchronization or timekeeping. The next generation of crosslinks will enable the space-infrastructure-as-a-service (SIAAS) paradigm in which separate vehicles will be able to exchange payloads with each other.

While we focus on conventional radio frequency crosslinks for the utility of this study, there have been extensive advancements in recent years for the integration of optical crosslinks into constellations [22]. Optical crosslinks leverage laser beams to exchange data between satellites, offering a wide range of advantages such as lower power requirements and higher data rates. However, the adoption of optical crosslinks in satellite constellations is still nascent and requires significant technological advancements to make it deployable at scale. Radio frequency is the primary medium for crosslinks today and is expected to remain in use by commercial and government entities for at least the next two decades.

Chapter 2
Motivation: Why Satellite Constellations?

2.1 Overview

The space technology and infrastructure industries are expected to boom in the coming decades as the barrier to space is increasingly dwindling. Ensuring that this next generation of space technology and infrastructure is hardened from potential cyber-threats will be a primary concern for cybersecurity specialists and aerospace engineers alike. The gamut of space technology and infrastructure spans wide, with new assets and architectures being continually developed. This chapter defends this thesis' efforts to prioritize allocating resources to secure satellite constellations in comparison to other space technologies and architectures.

2.2 Groundwork and Hybrid Architectures

The next generation of space infrastructures and architectures will require the capability to perform robust inter-agent communications and/or transactions. This can range from refueling to OSAM and ISAM (see figure 4). Without this functionality, architectures will sacrifice both efficiency and potential security benefits. Much of this inter-agent functionality will come from the aforementioned SIAAS paradigm which will enable the sharing of hosted payloads across vehicles. From a technical standpoint, the fundamental capability/technology which enables this inter-agent communication is

crosslinks. The contemporary point of reference for the utilization of crosslinks are satellite constellations. Thus, by performing robust research on hardening satellite constellations from cyberattacks (with particular focus on mitigating malware propagation), this will provide utility across the full gamut of next-generation space technologies and architectures. It can subsequently be asserted that amongst the array of existing space-based architectures, satellite constellations will be the most deployed. By extension, satellite constellations will increasingly begin to integrate with critical infrastructure. Thus, it is paramount that efforts and resources are allocated to bolstering the security and subsequent availability of satellite constellations.

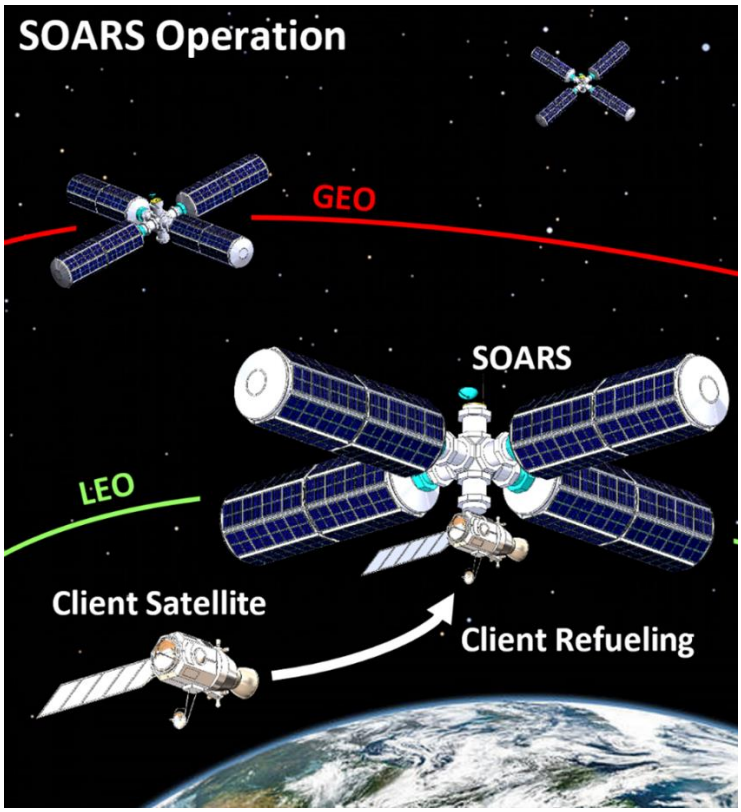

Figure 4. Example of Crosslink Utilization in Next-generation Space Architectures [24]

2.3 New Concerns

Cybersecurity concerns for satellites have for the most part been fixated on ensuring confidentiality. Thus, it is common for critical satellites to encrypt space-to-ground traffic. While there have been recent efforts to ensure the integrity and availability of satellites through basic defense mechanisms such as authentication, these efforts are still nascent. As space-based assets transition into playing roles in inter-agent systems, this paradigm will bring forth a new array of cybersecurity threats. Primarily, the danger of computer worms (self-propagating malware) infecting an entire constellation through the breach of a singular vehicle (SPOF) is a major threat. Cyber-threats brought forth by this inter-agent paradigm have yet to be explored in depth, hence the motivation for this thesis. By obtaining a more robust understanding of the potential damages a malicious cyber-actor can inflict across a constellation by compromising a singular satellite, further awareness will be brought to this issue. Moreover, outlining and studying a hacker's potential attack procedure will further optimize the development of defenses.

Chapter 3

Literature Review

3.1 Previous Work

This section will adumbrate the findings and understandings gleaned from existing literature.

3.1.1 Legislation

Unique to space-based assets, once deployed, engineers and operators are unlikely to have physical access to hardware again. This lack of access to the satellite highlights the need to implement modern and cutting-edge security measures [25]. Offensive cybersecurity is a highly dynamic arena, with innovative attack methodologies continuously being developed. Failure to adopt the latest security mechanisms, research, and protocols will result in an obsolete defense architecture and a consequent rapid accumulation of vulnerabilities. Unfortunately, cybersecurity is seldom a component of satellite risk assessments. This is however incongruous when it comes to our nation's critical space infrastructure. This is evident with the establishment of the United States Space Force (USSF) on December 30th, 2019, which—amongst other obligations—sought to harden the military's satellite network security. Recognition only continues to grow with President Biden's $773 billion budget request for the Defense Department in

FY 2023 [26]. This includes $24.5 billion for the U.S. Space Force and the Space Development Agency—about $5 billion more than what Congress enacted in 2022 [26].

From the standpoint of legislation, however, the United States has been sluggish in combating the plight of vulnerable space-based assets playing roles in critical infrastructure. As delineated in the Defense Space Strategy, the United Kingdom has already defined space as a part of their critical national infrastructure (CNI) [27]. The United States has only recently initiated the effort to mimic this initiative, through CISA's formation of the Space Systems Critical Infrastructure Working Group. As claimed by CISA, "this working group serves as an important mechanism to improve the security and resilience of commercial space systems. It will identify and offer solutions to areas that need improvement in both the government and private sectors and will develop recommendations to effectively manage risk to space based assets and critical functions. The Working Group will operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, bringing together space system critical infrastructure stakeholders". Since the group's establishment in May of 2021, significant advancements have yet to been made in the designation of space systems as one of CISA's critical infrastructures (currently 16) [4]. If achieved, this will greatly facilitate the effort to harden satellite constellations, with significant funding being allocated from critical infrastructure bills.

Conversely from a commercial standpoint, government agencies such as the NSA and CISA have actively focused resources on publishing satellite security advisories for vendors. This ranges from protocols to secure very small aperture terminal (VSAT)

networks to mitigations for SATCOM network providers and customers [28] [29]. In fact, on June 21st, 2022, senator Gary C. Peters, amongst the Homeland Security and Governmental Affairs committee, introduced the Satellite Cybersecurity Act vowing for CISA to maintain a publicly available clearinghouse of resources concerning the cybersecurity of commercial satellite systems [30]. As reported by [31], CISA would also be required to "consolidate voluntary recommendations for the development, maintenance, and operation of such systems. The recommendations are to include measures to protect systems against cyber-related vulnerabilities, risks, and attacks. To the extent practicable, CISA must implement its activities as a public-private partnership. The bill also requires the Government Accountability Office (GAO) to study and report on (1) federal actions to support the cybersecurity of commercial satellite systems, including with respect to critical infrastructure sectors; and (2) federal reliance on such systems, including those owned or controlled by foreign entities. In carrying out its study and report, the GAO must coordinate with designated federal agencies" [31]. While only introduced and yet to be passed by the senate, initiating official legislation will significantly bolster the awareness of this issue and will serve as a steppingstone for further governmental regulation.

3.1.2 COTS Employment in Satellites and DEVSECOPS Concerns

The DEVSECOPS concerns of COTS components have been extensively emphasized by CISA. Amongst the lengthy enumeration of security concerns, CISA states that "COTS products are generally black boxes to their customers. They can review

neither the code nor the architecture. In general, COTS buyers have to rely on the reputation of the developers, published security reports, and security forums. Many software vendors provide public assertions of their security, but these are rarely specific or quantitative. Vendors publish little or nothing about their coding practices as they relate to security. Installation manuals for COTS products are also light on discussions of security" [32]. Apart from the customers of COTS products not being able to review the code for security concerns, it can also be assumed that COTS manufacturers are not sifting through numerous lines of code for the sake of security. This is in part due to the fact that COTS software vendors have very limited liability. In the context of COTS, CISA states "among many product categories, there is established legal precedence for product vendors being held liable for the direct and even consequential damages resulting from the failure of their products and sometimes even damages resulting from misuse, particularly when that misuse is not explicitly proscribed. This is not the case with software. Virtually all software comes with a user agreement that explicitly absolves the software vendor of any liability, direct or consequential, even if that failure is a consequence of a known flaw in the product. To use the software, the customer must agree to these terms, and, in general, affected customers have not pursued legal remedies when software has failed" [32]. The succeeding language is extracted from an online legal document provided as a model for software product liability. It is consistent with the agreements from several major vendors [32]. "To the full extent permitted by law, [Vendor] is not liable for any direct, indirect, punitive, incidental, consequential, or exemplary damages (including without limitation loss of business, revenue, profits, goodwill, use of system, or other economic advantage) as a result of or in connection

with this software, even if [Vendor] has knowledge of or could reasonably have foreseen the possibility of such damages, however they arise" [32]. Thus, it can be asserted that satellites are at heightened risk for DEVSECOPS-originating vulnerabilities in comparison to conventional systems.

3.1.3 Attack Vectors in Satellites

There are a variety of attack vectors that can be exploited to inject malware into a satellite. These attack vectors can be classified into the three conventional satellite segments: the space segment, user segment, and ground segment. Each segment bears its own set of potential vulnerabilities and susceptibility to specific cyber-threats.

The space segment is the hardest to breach directly as it requires bypassing any potential on-board authentication. However, there are vectors that can be exploited to cause damage that is cyber-physical in nature. The primary attack vector for the space segment is the command ingest software application which is responsible for receiving commands and then sending them to the CDHS for handling. If this application is breached and is altered to pass a specific command to the CDHS, a malicious actor could gain administrative control over the satellite. Malicious actions could range from driving the asset out of orbit to pointing its solar panels towards the sun.

There are far fewer barriers to the ground segment in comparison to the space segment. To breach a ground station a malicious actor could take a conventional offensive security approach as seen with standard computers. Ground stations are often operated by either a single or set of computers that run a conventional operating system

such as Windows OS, Linux, or MacOS. Thus, attack vectors for the ground segment are primarily associated with this operating computer. Akin to a conventional computer, attack vectors would either be through the user running the system, the computer's connection to the internet/intranet, or through an external peripheral. A plausible attack scenario would be delivering a spear phishing email to the user account on the computer running the ground station. This email could trick the operator into running malware that uplinks a malicious command to the satellite.

In contrast to the ground segment, the user segment generally does not bear uplink capabilities. As a result, there is no way to directly affect the functionality of the satellite by breaching the user segment. However, there is still potential malicious activity that could be inflicted. For instance, malicious actors could conduct a man-in-the-middle attack to violate the integrity of data that is being downlinked from the satellite. The attack vectors for the user segment are often easier to exploit in comparison to other segments, as users are the most vulnerable component of a system.

3.1.4 Cyberattacks Against Satellites

Due to the sensitive nature of this subject, there have not been many publicly disclosed incidents of cyberattacks against space systems. As a result, there is a significant gap of literature in this subject. Despite this void in literature, current trends affirm that cyber-ASATs will threaten the foundations of space's longstanding stability due to their high accessibility, low attributability, and low risk of collateral damage [33]. Major non-kinetic attacks on satellites that are both publicly available for scrutiny and are

recent in nature are highlighted as follows. It is emphasized that these incidents are not exhaustive in order to provide an accurate depiction of the current threat landscape.

The Russo-Ukraine war has shed significant light on the subject of space cybersecurity. This is primarily due to the operation of SpaceX's Starlink, which enabled Ukrainian civilians to leverage the technology for communication purposes. As stated by Ruters, SpaceX privately shipped truckloads of Starlink terminals to Ukraine, enabling the country's military to communicate by plugging them in and connecting them with the nearly 4,000 satellites SpaceX had launched into LEO [34]. However, it was later reported by SpaceX founder Elon Musk that Russia had jammed Starlink terminals in the country for hours at a time [35]. While SpaceX was able to push a patch that prevented further jamming, it served as a major incident of a non-kinetic attack against a satellite. Jamming satellites and subsequent radio equipment is not a novel method of malicious non-kinetic activities, however, this incident provides further context in the domain of satellite constellation security.

Viasat is a satellite communication service provider that experienced an outage of its KA-SAT Network on February 24, 2022. As reported in [36] thousands of end-user terminals were disabled due to a wiper malware. This prevented a multitude of users from connecting to the network without subsequent replacement of the modem. [36] claims that this attack stands as the most significant publicly disclosed attack against a space system in recent history and is the first instance of a cyberattack serving as a first digital strike in a military conflict, occurring just an hour before the Russian invasion of Ukraine in February of 2022.

In November of 2014, NOAA revealed a breach of a satellite system by nation-state actors that were believed to be from China. Allegedly, the attackers were able to gain access to the satellites command and control (C2) system and uplink commands that caused the satellite to go offline [37]. As a result, NOAA was forced to discontinue the release of public satellite imagery from its website for over a week [37]. Specific details as to the attack vector and subsequent means of the breach were not disclosed.

3.1.5 Inter-Satellite Link Security

There have been no public disclosures of a cyberattack that exploited crosslinks to inflict damage. However, there has been recent attention regarding the threat of malware propagation across this medium. [38] explores this subject extensively with a particular focus on the potential damage that will be incurred if malicious actors are able to gain administrative control over a satellite with crosslink capabilities. Potential consequences asserted include damaging radio frequency actuators as well as electromagnetic pulse actuators. To conduct this operation, malware could be propagated that causes the victim satellite to not reach its desired location by tricking the victim into believing that it has already reached its orbit. Alternatively, attackers could trick a victim satellite into using its propulsion to deorbit by falsely representing that the victim is in the wrong location [38]. [38] also states that assuming an offensive satellite can maneuver itself to deliver a line-of-sight attack to a victim, EMP actuators could be exploited. Such capabilities are already in development by companies such as True Anomaly, who are engineering

technical capabilities needed to conduct adversarial rendezvous proximity operations [39].

[40] highlights potential cybersecurity vulnerabilities and pitfalls specific to satellite constellations. These vulnerabilities and pitfalls are highlighted as follows. First, some constellations may employ random routing protocols to assist in determining the most optimal crosslink to send traffic on to reach its intended destination. This lack of a single point of control may prevent deploying traditional defensive measures.

Also highlighted is the danger of the trusting of various ground stations to enable operations. Some constellation paradigms operate in a many-to-many relationship in that each satellite and ground station will bear bidirectional capabilities. This is in contrast to other satellite constellation architectures that have a singular entity that is responsible for communication with the ground station. Adopting the many-to-many relationship within a constellation requires a larger network of ground stations that must be appropriately documented for subsequent authentication. Introducing this larger ecosystem ultimately expands the attack surface for the breach of a satellite.

[41] poses a novel approach to securing inter-satellite links through the integration of blockchain technology. Specifically, a new concept dubbed the “Space Digital Token” (SDT) is proposed (see figure 5). SDT functions by tokenizing space transactions as digital tokens that can be processed using a blockchain protocol for authenticating space transactions. Hence, this technology serves as a mediator or authenticator for all communication patterns that occur within the satellite’s constellation. SDT also bears the capability to process sensor data between satellites and orbital debris.

Thus, it can serve as a tracking system for detecting expected space collisions between satellites and orbital debris. SDT bears the potential to be a highly promising solution especially for those that seek to adopt the SIAAS paradigm.

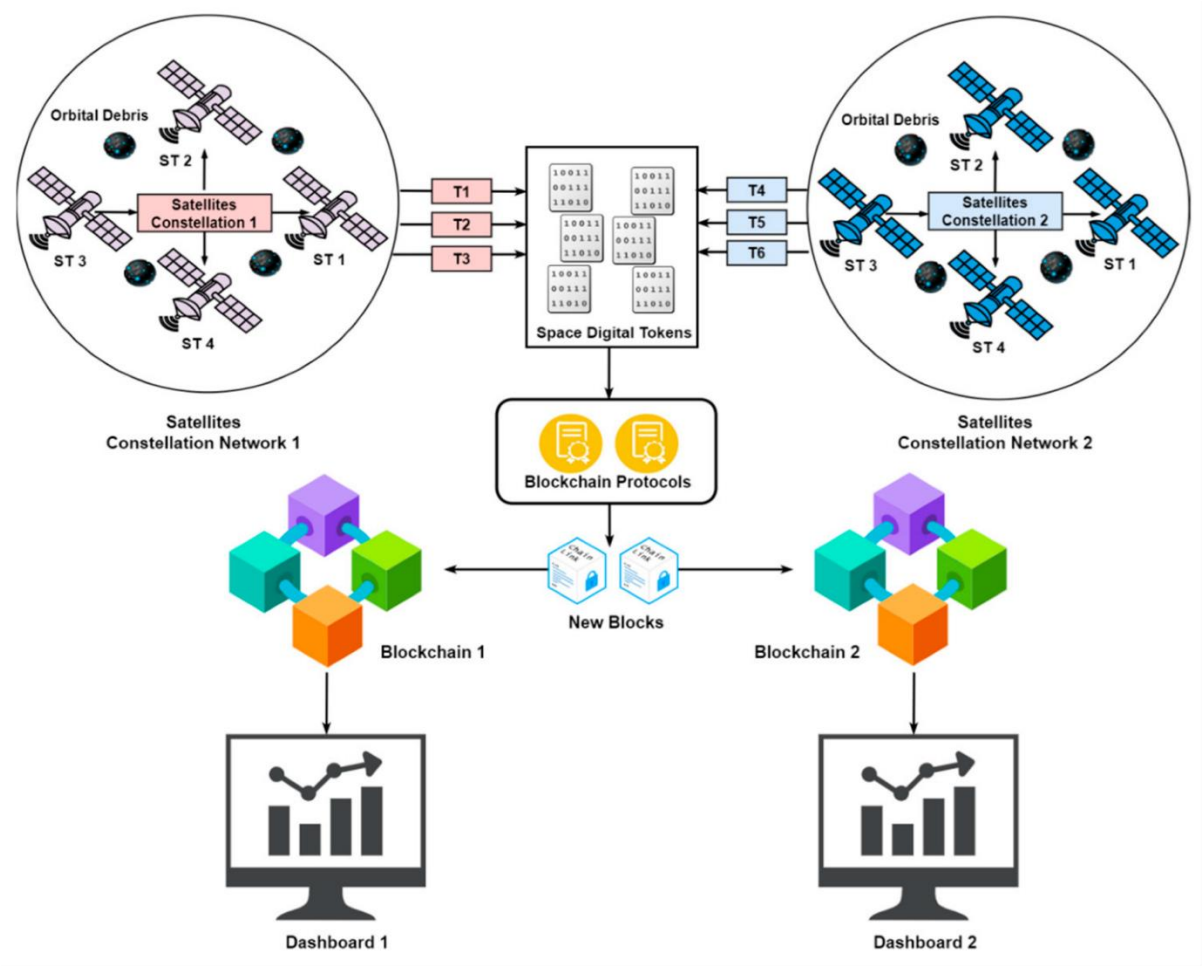

Figure 5. Space Digital Token Overview [41]

3.2 Limitations of Previous Work and Newly Proposed Research

Existing literature, while scanty, serves as a sufficient driver for the potential dangers that the exploitation of an inter-satellite link can cause. However, there are multiple limitations in this set of literature that prompt further study into this subject.

Identifying potential vulnerabilities in satellite constellations and impacts that malicious actors can cause does hold some utility in this domain. Primarily, it serves as an optimal reference for those that seek to engineer defenses for crosslinks. However, as previously mentioned, merely enumerating these threats and devising potential solutions will not hold any utility in either the commercial or government space sector. Researching, developing, and ultimately integrating security solutions for space systems requires extensive resources. Such resources cannot be simply allocated on the whim and will require significant advocation for the issue at hand. Thus, in a resource constrained domain there must be sufficient demonstrations of viability that will outweigh any potential concerns. The introduction of this thesis refers to the alleged exigent threat of quantum-enabled cyberattacks towards satellites in this regard. To remediate this lack of demonstration, the succeeding chapters will demonstrate the technical capability for malicious actors to exploit satellite-to-satellite crosslinks via cyber-ASAT weapons.

There is also an overall lack of study on the potential danger of cascading failures occurring to an entire constellation as a result of a singular breach of a vehicle. While this may be in part due to the lack of public disclosure regarding the networking architectures within constellations (for security reasons), the omission or lack of specificity regarding this concern detracts from the utility of these studies.

In reference to [41], which proposes a blockchain solution for implementing secure exchange of data across vehicles, there are potential limitations. Namely, the necessary computational power to implement such a technology may exceed what is acceptable for commercial entities. Due to the limited computational power of a satellite, there is little wiggle room for the contents of the payload. If this technology is adopted, an engineer would have to potentially deduct in a computational capacity from their mission payload to allot sufficient power for the SDT. While public sectors could be expected to compromise to these adjustments, this cannot be assumed for the private sector. As seen in the cybersecurity landscape of the private sector, many are willing to sacrifice extra security in return for a more optimized end-user experience. It is expected that this attitude towards cybersecurity in the private sector will manifest in the space domain. Therefore, satellite payload engineers will be reluctant to implement computationally expensive security algorithms if it will deduct from the potency of their payload. Thus, a challenge exists to ensure that the security apparatus is computationally resourceful enough to not detract in a significant manner from the mission payload. Potential solutions include integrating lightweight blockchain technologies optimized to function at the edge as demonstrated in [42]. To ensure the initial steps are taken to address the threat of crosslink exploitation as a mechanism for malware propagation, this thesis will propose simple and first steps that should be taken. In addition, potential R&D endeavors to undertake which will provide utility for the mitigation of this threat will also be proposed.

Chapter 4

Methodology and Experimental Design

4.1 Overview

A primary objective of this thesis is to demonstrate the technical capability for malicious actors to employ cyber-ASAT capabilities to exploit vulnerabilities in satellite-to-satellite crosslinks. In addition, this thesis seeks to highlight the potential consequences of a successful attack execution. This chapter details the experimental approach undertaken to satisfy these objectives.

4.2 Methodology

To perform this demonstration, a network of three satellites interconnected by radio frequency crosslinks and a singular ground station was emulated. This emulation was subsequently penetration tested to exhibit the capability for a malicious actor to exploit an ISL for malware propagation. Three total attacks were demonstrated. First, a conventional cyber-physical attack was performed to demonstrate the feasibility for a satellite to cause physical damage to a cross-linked satellite without intermediary communication from a ground station. Next, a spoofing attack was demonstrated in which an adversarial vehicle falsified its identity to receive communications from a benign satellite (via crosslink) within a constellation. Finally, the procedure for a side channel attack was demonstrated in which a malicious vehicle equipped with a spectrum

analyzer payload assessed electromagnetic radiation emitted between two satellites communicating via crosslink to glean potentially exploitable communication information. The motive behind each attack is further delineated in the experiment subsection.

4.2.1 Justification and Reasoning

As mentioned in preceding chapters, there is an existing void in literature of attack demonstrations against inter-satellite links. An experimental method of research (emulation and penetration testing) was therefore selected as it provides a concrete reference of feasibility for conducting a satellite-to-satellite cyberattack. This is in contrast to a quantitative, qualitative, or formal methods study which derives or asserts that the technical feasibility to conduct such an attack exists without demonstration.

There are a multitude of restrictions and barriers that hinder the ability to effectively demonstrate the technical feasibility of breaching a satellite constellation via cyberattack. These hinderances are primarily due to budgetary and legal complications. The radio frequency spectrum is highly critical and sensitive to a variety of operations. Inadvertently transmitting or tampering with the radio frequency spectrum will lead to legal trouble as asserted by the Federal Communications Commission (FCC). To avoid such troubles, this study was performed in a highly controlled capacity and required the omission of certain experiments which could hold great utility. It is therefore acknowledged that the replication of this study in an FFRDC environment will provide significant benefit.

4.3 Resources, Equipment, and Configuration

This section details the tools, resources, and equipment utilized to emulate the satellite constellation and perform the subsequent penetration test. Furthermore, it describes the process undertaken to configure this equipment and subsequent limitations.

4.3.1 Ground Station

To emulate a ground station, a standard laptop running Windows 11 with Arduino IDE was installed. To provide a method of interfacing with the satellites, a USB Hub splitter (5 ports) was utilized in addition to 3 USB 2.0 A/B cables. The USB A end was plugged into the USB Hub splitter and the B end was plugged into the satellite (see succeeding content). To emulate the process of uplinking a command or software payload, the uploading operation on the Arduino IDE was executed.

4.3.2 Satellite

Each satellite within the network was abstracted to an OBC and respective antenna for the purpose of this demonstration. To represent the OBC, an Arduino Uno was utilized. Each Arduino Uno (3x) received the B end of the USB 2.0 A/B cable to enable interface with the ground station.

To enable radio communications (for crosslink transmissions), each Arduino Uno was equipped with an nRF24L01 wireless transceiver radio frequency module. To account for regulator issues between the Arduino Uno and the nRF24L01 radio module, a

breakout adapter (3.3V) was connected as an intermediary. This ensured that the nRF24L01 radio module was safely engaging the Arduino Uno by regulating and stabilizing voltage in addition to facilitating the conversion of logic levels for signals.

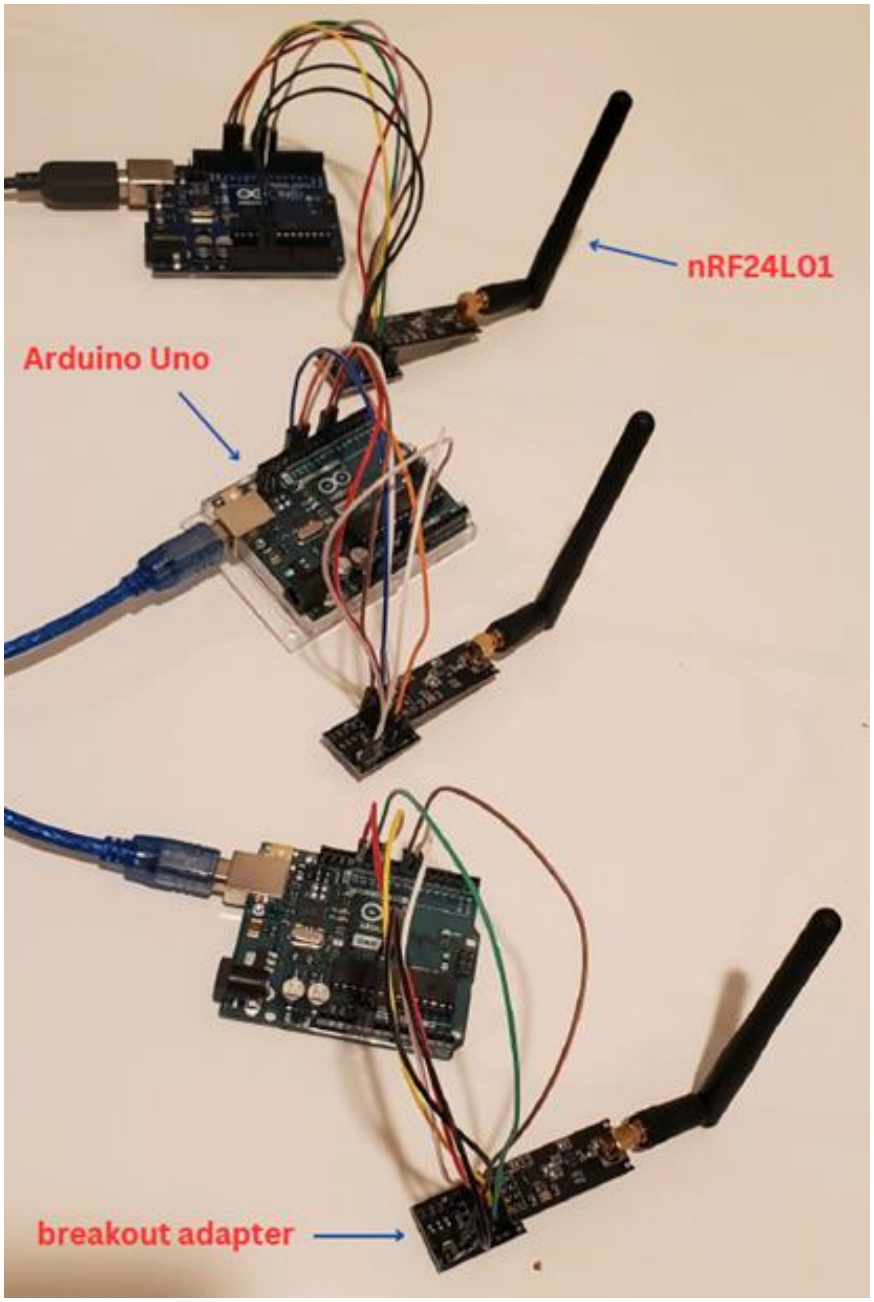

Figure 6. Satellite Constellation Emulation Setup

Male to female jumper cable wires (figure 7) were utilized to enable the nRF24L01 modules and subsequent breakout adapters to interface with the Arduino Uno. The same pinout was utilized for each demonstrated attack. This pinout is enumerated in table 1.

Figure 7. Male to Female Jumper Cable Wire

Table 1. Pinout for Arduino Uno and nRF24L01 Radio Module Breakout Adapter

ARDUINO PIN	BREAKOUT ADAPTER
12	M1
11	M0
13	SERIAL CLOCK (SCK)
8	CHIP SELECT NOT (CSN)
7	CHIP ENABLE (CE)
GROUND	GROUND
5 Volts (5V)	VOLTAGE COMMON COLLECTOR (VCC)

4.3.3 Malicious Spectrum Analysis Vehicle

To emulate a malicious vehicle equipped with a spectrum analyzer payload, a software defined radio (SDR) with a 180-degree dipole antenna was utilized (figure 8). The SDR was connected to the USB Hub Splitter and configured to function with SDRSharp. To perform spectrum analysis, SDRSharp was tuned to 2.4Ghz to eavesdrop on the communications between the Arduino Unos communicating via the nRF24L01 radio modules.

Figure 8. SDR Dipole Antenna

4.3.4 Abstraction Limitation

It is acknowledged that employing an Arduino Uno, nRF24L01 radio module, and an external SDR to abstract an in-orbit satellite is not optimal. While alternative resources with higher likeness exists, these resources were out of budget for this study. CubeSats (approximate price of $10,000 per unit) would hold particular utility in replicating this

study to account for these limitations. This presents potential complications with drawing concrete conclusions. Namely, satellites are composed of various subsystems as mentioned in 1.4.3. The execution of code by various actuators and subsystems is directed by the CDHS, which cannot be wholly emulated utilizing this setup. Malware in a real-world scenario would be written in C and tailored to the specific constellation. For instance, malware written for a satellite internet constellation may require further efforts to crawl into the CDHS. This is in contrast to a SIAAS operation which would most likely not require these changes. Table 2 depicts the relationship between the emulation utilized for this study and a real-world satellite-to-satellite crosslink. Drawn conclusions from this study should be cognizant of these limitations.

Table 2. Relationship Between Emulation and Real-World Crosslinked Satellites

Emulation	Real-World Crosslinked Satellite
Arduino UNO	OBC
PIN 13 LED	Mechanical Actuator (RF, EMP, etc)
nRF24L01 radio module	Antenna
Transmitting Code	Modulator [Software Bus]
Receiving Code	Command Ingest [Software Bus] [CDHS] [Demodulator]
SDR	In-situ GPU + External Antenna [Spectrum Analysis]

4.4 Experiment

This section details the procedure and execution of the penetration test. Furthermore, the justification behind selecting each attack type is delineated.

4.4.1 Cyber-Physical Attack

Stuxnet--a notorious worm that breached the Iranian nuclear program--functioned by breaching programmable logic controllers (PLCs) to manipulate the speed of centrifuges and cause physical damage to equipment. Similarly, the feasibility exists for a satellite to inflict cyber-physical damage to another satellite through the exploitation of crosslinks. Demonstrating this feasibility was the primary purpose of emulating this attack. To perform this emulation, malware was written in Arduino (Appendix A) to propagate from one satellite to another via the established nRF24L01 crosslink. Akin to Stuxnet, this malware was tasked with excessively modulating the PLC (pin 13 | LED) to cause “physical damage”. Due to the limitations of this study, pin 13 was selected to conduct the attack to prevent physical damage to the Arduino Uno board and respective peripherals. In an uncontrolled and real-world setting, however, this attack would excessively modulate EMP and RF actuators aboard the satellite as mentioned in [38] as well as peripherals such as robotic arms. To uplink the malware, the Arduino code was uploaded and transmitted using Arduino IDE to the first satellite via the USB splitter and then propagated to the victim satellite using the nRF24L01 crosslink.

4.4.2 Spoofing Attack

As highlighted in [40] it is often that robust authentication mechanisms are not employed for crosslink transmissions within a satellite constellation. To demonstrate the feasibility for a malicious actor to exploit this decision, a spoofing attack is conducted. Three satellites were first configured with crosslink capabilities. Arduino code was written to enable bidirectional transmissions between two satellites. This code was tasked with emulating a SIAAS operation, in which a proprietary software payload to enable a satellite to indicate its position through a beacon (turn on LED) was shared (Appendix B).

Malware was then written in Arduino (Appendix C) to emulate a malicious vehicle spoofing its identity as the benign receiver to steal the beacon payload. This malware was uploaded to the 3rd satellite (malicious vehicle) to enable ingress of the proprietary transmissions.

4.4.3 Side Channel Attack

Most orbiting satellites currently do not possess the capability to perform characterization or analysis of signals due to computational limits. However, such capabilities have been extensively explored in recent years as delineated in [43]. It should therefore be expected that on-board electromagnetic analysis capabilities will be a conventional payload for future adversarial space vehicles. This attack consequently sought to demonstrate the threat this advent will pose to satellite constellations.

To conduct this attack, the benign code utilized in the preceding attack (Appendix B) was uploaded to initiate communication between two satellites via crosslink. Following a connection of the SDR to the computer (ground station) and subsequent tuning of SDRSharp to 2.4Ghz, manual analysis of the electromagnetic radiation (as picked up by SDRSharp) was conducted. Analysis focused on identifying patterns and characteristics that could reveal information about the communication between the satellites to facilitate a jamming or replay attack. Due to the limitations of this study (legalities), the amplitude was recorded but was not subsequently exploited.

Chapter 5

Results and Discussion

5.1 Overview

This chapter will discuss the results and subsequent utility of the preceding experiments. In addition, potential solutions to counter these threats are discussed. Finally, limitations to this study as well as considerations for future work are delineated.

5.2 Cyber-Physical Attack Analysis

The cyber-physical attack emulation was successfully executed to demonstrate the technical feasibility of exploiting a satellite-to-satellite crosslink to deploy malware with cyber-physical damage capabilities. While this experiment was highly abstracted due to the limitations of this study, there are little to no further technical barriers to conducting such an attack in a real-world scenario. With sufficient engineering of worm propagation, there is a high likelihood that a malicious actor could deploy similar malware on a single vehicle within a constellation to cause physical damage to the rest of the vehicles within the network. To mitigate the threat of this attack, the following solutions are recommended. At a bare minimum, dual factor authentication as well as separation of duties should be implemented for critical uplinks from the ground station. While operators can decide on which suite of commands should be classified as critical, it is strongly recommended that this list includes the uplinking of software payloads.

Perhaps the most robust and long-term solution is to implement a zero-trust architecture as discussed in [44] in which stateful inspection is conducted for each transmission. Akin to a firewall which performs deep packet inspection (DPI), satellites within a constellation should bear the capability to distinguish between benign and malicious transmissions. While not extensively explored in literature for embedded systems, the employment of machine learning as described in [43] should provide significant benefit in reducing computational complexity as well as TNR and FPR. There are potential limitations for this approach, however. Namely, there may be an increase in latency which would be a major hinderance to those running time-critical services. Commercial vendors running satellite internet services such as SpaceX's Starlink may also object to such a solution due to visible latency issues.

5.3 Spoofing Attack Analysis

The spoofing attack was successfully executed as the malicious vehicle was able to spoof its identity as the benign receiver and ingress the proprietary payload. While this emulation was an abstraction of a conventional satellite-to-satellite transmission, conducting such an operation in an uncontrolled and real-world setting will require little to no further technical capabilities that were not demonstrated in this emulation. However, effective intelligence gathering is a pre-requisite to conducting this attack as the unique identifier and/or address of the benign receiver must be gleaned. Without the address of the benign receiver, a malicious actor will be unable to effectively execute the spoofing attack. It is also a requirement that the malicious vehicle bolsters an antenna

capable of overpowering the benign receiver. This ensures that the benign transmitter will identify the malicious vehicle as the intended receiver first. Based on the configurations and method of transmission, it is also possible that both the benign receiver and the malicious receiver will receive the transmission. Due to the configuration of this experiment, this scenario was not demonstrated.

There are multiple potential solutions to mitigate the effectiveness of such an attack. One potential solution is to implement asymmetric encryption and public key infrastructure. Each satellite within a constellation maintains a database or list containing unique identifiers and/or addresses for every vehicle in the network to enable routing. Thus, this unique identifier can serve as the public key. Subsequently, each satellite can be equipped with a private key which can be utilized to decrypt the transmissions. Thus, a malicious vehicle attempting to spoof as a benign entity within the constellation will be unable to do so as the private key will be required to decrypt and utilize the payload. There is a potential limitation to this study. Namely, if vendors decide to leverage homomorphic encryption—which would hold significant utility for SIAAS operations—then there would be no means of in situ verification of identity. This of course could be remediated by encrypting the transmissions using asymmetric encryption and then subsequently processing it utilizing homomorphic encryption to avoid revealing the underlying makeup of the payload.

5.4 Side Channel Attack Analysis

The side channel attack was successfully executed as the malicious vehicle was able to exploit the EMR of the communications between two satellites to glean the amplitude. While this attack was abstracted due to limitations, it serves as a demonstration of the technical feasibility for malicious actors to employ spectrum analysis payloads as delineated in [43] to compromise satellites communicating via crosslink. A recognized hinderance of this experiment is that the spectrum analysis was conducted manually (not autonomously). Thus, to ensure the viability of this experiment, only the amplitude was recorded. While full-scale spectrum analysis payloads capable of gleaning all the information needed to conduct a replay or jamming attack have not been publicly deployed, recording the amplitude is currently feasible. With this information, characteristics such as signal strength and modulation schemes (i.e.: amplitude shift keying or frequency-shift keying) could be recorded to ultimately facilitate conducting a successful replay or jamming attack. It is also noted that conducting this attack in a real-world scenario may require the malicious vehicle to conduct a rendezvous proximity operation in order to optimize the gleaning of EMR between the two satellites. While this maneuver is not required, it would significantly bolster the effectiveness of the attack.

There are various ECCMs that can be integrated into the satellites within a constellation to hinder adversarial spectrum analysis. At a bare minimum, encryption should be applied for all satellite-to-satellite transmissions. This will prevent identifying the amplitude, however, characteristics such as bandwidth, frequency, and timing may still be gleaned. Basic frequency modulation security measures can help in this regard,

such as the FHSS. To counter potential fast-follower electronic weapons, there are potential applications of machine learning as delineated in [3]. Identifying and recovering from a jamming attack will require in-situ capabilities to characterize radio frequency signals as discussed in [43] and identification of variables indicative of such attacks (i.e.: high noise floor, bit error rate, and lack of control channel) as enumerated in [3].

Chapter 6

Conclusion

This thesis experimentally demonstrated the technical feasibility for malicious actors to exploit satellite-to-satellite crosslink capabilities through the deployment of cyber-ASAT weaponry. Insight was brought to the devastating effects that worm propagation throughout a satellite constellation would cause. Potential solutions to thwart these consequences were subsequently delineated. While legal ramifications and budgetary restrictions caused limitations for this research, I am confident that it possesses the capability to serve as a reference for the viability of a satellite-to-satellite cyberattack. Replication of this study in an FFRDC environment with a more robust testbed will hold significant utility in remediating the limitations of this research. As the number of operational satellite constellations surges in the coming decades, it is paramount that appropriate measures are taken to address the concerns addressed in this thesis. Failure to do so will result in irreversible damage.

Appendix A

Cyber-Physical Attack Code

```
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
RF24 radio(7, 8); // CE, CSN pins
const byte address[6] = "00001";
void setup() {
  Serial.begin(9600);
  radio.begin();
  radio.openWritingPipe(address);
  radio.setPALevel(RF24_PA_MAX);
  radio.setDataRate(RF24_250KBPS);
  radio.setChannel(110);
  radio.setCRCLength(RF24_CRC_16);
  radio.setAutoAck(1);
}

void loop() {
  radio.write("LED ON", sizeof("LED ON"));
```

```
  delay(1000);
}
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
RF24 radio(7, 8); // CE, CSN pins
const byte address[6] = "00001";

void setup() {
  Serial.begin(9600);
  radio.begin();
  radio.openReadingPipe(0, address);
  radio.setPALevel(RF24_PA_MAX);
  radio.setDataRate(RF24_250KBPS);
  radio.setChannel(110);
  radio.setCRCLength(RF24_CRC_16);
  radio.setAutoAck(1);
  pinMode(LED_BUILTIN, OUTPUT);
}

void loop() {
  while (radio.available()) {
    char message[6];
```

```
    radio.read(message, sizeof(message));
    if (strcmp(message, "LED ON") == 0) {
      digitalWrite(LED_BUILTIN, HIGH);
      delay(50);
      digitalWrite(LED_BUILTIN, LOW);
      delay(50);
    }
  }
}
```

Appendix B

Spoofing Attack Code (Benign Beacon Payload Transfer)

```
#include <SPI.h>

#include <nRF24L01.h>

#include <RF24.h>


RF24 radio(7, 8); // CE, CSN pins


const byte address[6] = "00001";


void setup() {

  Serial.begin(9600);


  radio.begin();

  radio.openWritingPipe(address);

  radio.setPALevel(RF24_PA_MAX);

  radio.setDataRate(RF24_250KBPS);

  radio.setChannel(110);

  radio.setCRCLength(RF24_CRC_16);

  radio.setAutoAck(1);

}
```

```
void loop() {
  radio.write("LED ON", sizeof("LED ON"));
  delay(1000);
}
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
RF24 radio(7, 8); // CE, CSN pins
const byte address[6] = "00001";
int ledPin = 13;
void setup() {
  Serial.begin(9600);
  radio.begin();
  radio.openReadingPipe(1, address);
  radio.setPALevel(RF24_PA_MAX);
  radio.setDataRate(RF24_250KBPS);
  radio.setChannel(110);
  radio.setCRCLength(RF24_CRC_16);
  radio.setAutoAck(1);
  radio.startListening();

  pinMode(ledPin, OUTPUT);
}
void loop() {
  if (radio.available()) {
```

```
    char message[8];
    radio.read(message, sizeof(message));
    if (strcmp(message, "LED ON") == 0) {
      // Turn on the LED
      digitalWrite(ledPin, HIGH);
    } else {
      // Turn off the LED
      digitalWrite(ledPin, LOW);
    }
  }
}
```

Appendix C

Spoofing Attack Code (Malicious Vehicle Identity Falsification)

```
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
RF24 radio(7, 8); // CE, CSN pins
const byte address[6] = "00001";
void setup() {
  Serial.begin(9600);

  radio.begin();
  radio.openWritingPipe(address);
  radio.setPALevel(RF24_PA_MAX);
  radio.setDataRate(RF24_250KBPS);
  radio.setChannel(110);
  radio.setCRCLength(RF24_CRC_16);
  radio.setAutoAck(1);
}
void loop() {
  radio.write("LED ON", sizeof("LED ON"));
  delay(1000);
```

```
}
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
RF24 radio(7, 8); // CE, CSN pins
const byte address[6] = "00001"; //spoofed address replicate
int ledPin = 13;
void setup() {
  Serial.begin(9600);
  radio.begin();
  radio.openReadingPipe(1, address);
  radio.setPALevel(RF24_PA_MAX);
  radio.setDataRate(RF24_250KBPS);
  radio.setChannel(110);
  radio.setCRCLength(RF24_CRC_16);
  radio.setAutoAck(1);
  radio.startListening();

  pinMode(ledPin, OUTPUT);
}
void loop() {
  if (radio.available()) {
    char message[8];
    radio.read(message, sizeof(message));
    if (strcmp(message, "LED ON") == 0) {
```

```
      // Turn on the LED
      digitalWrite(ledPin, HIGH);
    } else {
      // Turn off the LED
      digitalWrite(ledPin, LOW);
    }
  }
}
```

BIBLIOGRAPHY

[1] “Never a day without space commander’s strategic vision,” USSPACECOM.

[2] “CISA Launches a Space Systems Critical Infrastructure Working Group | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, May 13, 2021. https://www.cisa.gov/news-events/news/cisa-launches-space-systems-critical-infrastructure-working-group

[3] R. K. Thummala and P. Liu, “Exploring the Applications of Frequency Modulation to Secure CubeSats from Eavesdropping, Jamming, and Interference,” in *ASCEND 2022*, Las Vegas, Nevada & Online, Oct. 2022. doi: 10.2514/6.2022-4381.

[4] “HOUSE SCIENCE, SPACE AND TECHNOLOGY COMMITTEE SUBCOMMITTEE ON SPACE AND AERONAUTICS JULY 28, 2022 WRITTEN TESTIMONY FOR DR. THERESA SULOWAY, MITRE CORPORATION.” [Online]. Available: https://republicans-science.house.gov/2022/7/exploring-cyber-space-cybersecurity-for-civil-and-commercial-space-systems

[5] A. Boyd, “Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army.” [Online]. Available: https://apps.dtic.mil/sti/citations/AD1038881

[6] P. Van Ness, “The Time Has Come for a Treaty to Ban Weapons in Space,” *Asian Perspective*, vol. 34, no. 3, pp. 215–225, 2010. [Online]. Available: https://www.jstor.org/stable/42704727

[7] “Outer Space Treaty May Ban Strike Weapons | Arms Control Association.” https://www.armscontrol.org/act/2002-06/outer-space-treaty-may-ban-strike-weapons

[8] T. W. House, “FACT SHEET: Vice President Harris Advances National Security Norms in Space,” *The White House*, Apr. 19, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/

[9] “Geostationary Satellites,” *National Environmental Satellite, Data, and Information Service*. https://www.nesdis.noaa.gov/current-satellite-missions/currently-flying/geostationary-satellites

[10] mars.nasa.gov, “Command & Data-handling Systems - NASA.” https://mars.nasa.gov/mro/mission/spacecraft/parts/command/

[11] J. F. News E&E, “Meet the Satellites That Can Pinpoint Methane and Carbon Dioxide Leaks,” *Scientific American*. https://www.scientificamerican.com/article/meet-the-satellites-that-can-pinpoint-methane-and-carbon-dioxide-leaks/

[12] D. W. Hafemeister, “Infrared monitoring of nuclear power in space,” *Science & Global Security*, vol. 1, no. 1–2, pp. 109–128, Jan. 1989, doi: 10.1080/08929888908426326.

[13] R. P. Sishodia, R. L. Ray, and S. K. Singh, “Applications of Remote Sensing in Precision Agriculture: A Review,” *Remote Sensing*, vol. 12, no. 19, p. 3136, Sep. 2020, doi: 10.3390/rs12193136.

[14] “Iridium,” *Gunter’s Space Page*. https://space.skyrocket.de/doc_sdat/iridium.htm

[15] “The Disaster Monitoring Constellation | Small Satellite supplier | Surrey Satellite Technology Ltd | SSTL.” https://www.sstl.co.uk/space-portfolio/the-disaster-monitoring-constellation

[16] P. B. de Selding, “SpaceX To Build 4,000 Broadband Satellites in Seattle,” *SpaceNews*, Jan. 19, 2015. https://spacenews.com/spacex-opening-seattle-plant-to-build-4000-broadband-satellites/

[17] “Telesat Begins Deploying Its Global Low Earth Orbit (LEO) Constellation with Successful Launch of Phase 1 Satellite | Telesat,” Jan. 12, 2018. https://www.telesat.com/press/press-releases/telesat-begins-deploying-its-global-low-earth-orbit-leo-constellation-with-successful-launch-of-phase-1-satellite/

[18] J. Porter, “Amazon will launch thousands of satellites to provide internet around the world,” *The Verge*, Apr. 04, 2019. https://www.theverge.com/2019/4/4/18295310/amazon-project-kuiper-satellite-internet-low-earth-orbit-facebook-spacex-starlink

[19] “Jonathan’s Space Report | Space Statistics.” https://planet4589.org/space/con/star/stats.html

[20] M. S. Petrova Magdalena, “Why in the next decade companies will launch thousands more satellites than in all of history,” *CNBC*, Dec. 15, 2019. https://www.cnbc.com/2019/12/14/spacex-oneweb-and-amazon-to-launch-thousands-more-satellites-in-2020s.html

[21] T. Pultarova, E. H. from A. Mann, and D. D. last updated, “Starlink satellites: Everything you need to know about the controversial internet megaconstellation,” *Space.com*, Apr. 14, 2022. https://www.space.com/spacex-starlink-satellites.html

[22] S. Erwin, “DoD to test laser communications terminals in low Earth orbit,” *SpaceNews*, Jun. 08, 2020. https://spacenews.com/dod-to-test-laser-communications-terminals-in-low-earth-orbit/

[23] “EarthSky | Starlink satellites can look like a plume or train of light,” Sep. 12, 2022. https://earthsky.org/space/spacex-starlink-satellites-explained/

[24] “Space Infrastructure,” *Zero-G Horizons Technologies*. https://www.zeroghorizons.com/space-infrastructure

[25] S. Kaczmarek, “Cybersecurity for Space Assets: Focusing on SmallSats and CubeSats,” *Sylvester Kaczmarek*, Jun. 06, 2021. https://sylvesterkaczmarek.com/blog/cybersecurity-for-space-assets-focusing-on-smallsats-and-cubesats/

[26] S. Erwin, “Biden’s 2023 defense budget adds billions for U.S. Space Force,” *SpaceNews*, Mar. 28, 2022. https://spacenews.com/bidens-2023-defense-budget-adds-billions-for-u-s-space-force/

[27] “Defence Space Strategy: Operationalising the Space Domain,” *GOV.UK*. https://www.gov.uk/government/publications/defence-space-strategy-operationalising-the-space-domain

[28] “NSA Issues Recommendations to Protect VSAT Communications,” *National Security Agency/Central Security Service*. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2910409/nsa-issues-recommendations-to-protect-vsat-communications/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F2910409%2Fnsa-issues-recommendations-to-protect-vsat-communications%2F

[29] “Strengthening Cybersecurity of SATCOM Network Providers and Customers | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, May 10, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a

[30] “ Sen. Peters, Gary C. Satellite Cybersecurity Act. 2022.” [Online]. Available: https://www.congress.gov/bill/117th-congress/senate-bill/3511

[31] “US Congress S3511.” [Online]. Available: https://trackbill.com/bill/us-congress-senate-bill-3511-a-bill-to-require-a-report-on-federal-support-to-the-cybersecurity-of-commercial-satellite-systems-and-for-other-purposes/2190849/

[32] “Security Considerations in Managing COTS Software.” [Online]. Available: https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

[33] J. Pavur and I. Martinovic, “The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space,” in *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, May 2019, pp. 1–18. doi: 10.23919/CYCON.2019.8756904.

[34] J. Roulette, “SpaceX curbed Ukraine’s use of Starlink internet for drones -company president,” *Reuters*, Feb. 09, 2023. [Online]. Available: https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/

[35] V. Insinna, “SpaceX beating Russian jamming attack was ‘eyewatering’: DoD official,” *Breaking Defense*, Apr. 20, 2022. https://breakingdefense.sites.breakingmedia.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/

[36] N. Boschetti, N. G. Gordon, and G. Falco, “Space Cybersecurity Lessons Learned from the ViaSat Cyberattack,” in *ASCEND 2022*, Las Vegas, Nevada & Online, Oct. 2022. doi: 10.2514/6.2022-4380.

[37] S. Bichler, “MITIGATING CYBER SECURITY RISK IN SATELLITE GROUND SYSTEMS ,” AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY . [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1012754.pdf

[38] G. Falco, “When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience,” in *ASCEND 2020,* Virtual Event, Nov. 2020. doi: 10.2514/6.2020-4014.

[39] M. Harris, “Enter the Hunter Satellites Preparing for Space War,” *Wired*. [Online]. Available: https://www.wired.com/story/true-anomaly-jackal-pursuit-satellites/

[40] V.-C. Matei, “Cybersecurity Analysis for the Internet-Connected Satellites ,” Upsala Universitet.

[41] M. Torky, T. Gaber, E. Goda, V. Snasel, and A. E. Hassanien, “A Blockchain Protocol for Authenticating Space Communications between Satellites Constellations,” *Aerospace*, vol. 9, no. 9, p. 495, Sep. 2022, doi: 10.3390/aerospace9090495.

[42] M. Zhang *et al.*, “Research on Lightweight Blockchain Technology Based on Edge Computing,” in *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, Jul. 2022, pp. 533–539. doi: 10.1109/DSC55868.2022.00080.

[43] G. Falco, N. G. Gordon, A. Byerly, A. Grotto, J. Siegel, and S. Zanlongo, “The Space Digital Dome: Autonomous Defense of Space Vehicles from Radio Frequency Interference,” in *2022 IEEE Aerospace Conference (AERO)*, Mar. 2022, pp. 1–8. doi: 10.1109/AERO53065.2022.9843425.

[44] M. M. / P. Jan 30 and 2023, “How ‘zero-trust’ could enable safe data exchange in space,” *The Hub*, Jan. 30, 2023. https://hub.jhu.edu/2023/01/30/zero-trust-space-marketplace/

ACADEMIC VITA

Rajiv Thummala

EDUCATION

The Pennsylvania State University – *University Park, PA* *May 2023*
Master of Science in Cybersecurity Analytics and Operations
[Integrated Undergraduate/Graduate (IUG) Program]

Schreyer Honors College (SHC) at Penn State – *University Park, PA* *May 2023*
Bachelor of Science in Cybersecurity Analytics and Operations

ACTIVITIES AND ORGANIZATIONS

National Security Club – Vice President [40+ members] *June 2022 – Present*
Everyday Benefitting Thon – Outreach Chair *August 2022 - Present*
HackPSU – Marketing Director *September 2020 – January 2022*
Competitive Cyber Security Organization – CCDC Selection *January 2021 – May 2021*

HONORS AND AWARDS

Phi Kappa Phi *March 2023*

- Invitation limited to the top 10% of the graduating class

Penn State College of IST Winter 2022 Standout Student *March 2022*

- Featured in the College of IST's semesterly magazine as a standout student

NASA Pennsylvania Space Grant Consortium Undergraduate Scholarship *May 2021*

- The 52 NASA consortia scholarships are a limited number of one-year scholarships are awarded to outstanding undergraduate students across the country who are enrolled in STEM programs and are likely to pursue a career in an area of interest to NASA

Dean's List *August 2019 - May 2023*

- All semesters

SELECTED PUBLICATIONS

R. K. Thummala and P. Liu, "Exploring the Applications of Frequency Modulation to Secure CubeSats from Eavesdropping, Jamming, and Interference," in *ASCEND 2022*, Las Vegas, Nevada & Online: American Institute of Aeronautics and Astronautics, Oct. 2022. doi: 10.2514/6.2022-4381.