TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Olena Roraff 201621IVGM

"CYBERSECURITY POLICY FOR THE SATELLITE INDUSTRY: GOVERNANCE CHALLENGES AND SOLUTIONS"

Master's Thesis

Supervisor: Paul Liias
Ph.D. Candidate
Co-Supervisor: Richard Dreyling
Ph.D. Candidate
Co-Supervisor: Eric Jackson
Ph.D. Candidate

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Olena Roraff 201621IVGM

“KÜBERTURVALISUSE POLIITIKA SATELLIIDITÖÖSTUSELE: VALITSEMISE RASKUSED JA -LAHENDUSED”

Magistritöö

Juhendaja: Paul Liias
Ph.D. Candidate
Kaasjuhendaja: Richard Dreyling
Ph.D. Candidate
Kaasjuhendaja: Eric Jackson
Ph.D. Candidate

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to the best of my knowledge and ability. This thesis has not been presented for examination anywhere else.

Author: Olena Roraff

09.05.2022

Abstract

The satellite communication industry is developing at a rapid speed. Satellite-enabled technologies are intertwined in the daily operations of governments, private companies, and citizens. It is important to ensure the resilience of the space infrastructure to continue to grow "the new space economy" and rely on secure satellite services to benefit all critical infrastructure sectors.

The study aims to determine how to improve the cybersecurity governance of the satellite industry at the policy level. Specifically, it investigates the current state of the U.S. cybersecurity regulations for the satellite industry and describes existing and perceived future cyber threats to satellite systems. In this context, the value of cyber exercise to inform policymaking processes is evaluated.

To test the hypothesis that cybersecurity governance of the satellite industry requires more attention and that cyber exercises can help strengthen that framework, several data collection activities were performed. Extensive regulatory analysis complemented by unstructured interviews and a survey were evaluated using qualitative methods of analysis.

The results suggest that the cybersecurity guidance should be better developed and specifically tailored to the unique requirements of satellite systems. The study concludes with actionable policy recommendations on the national and organizational levels to enhance the U.S. preparedness for a very real scenario of a cyber-attack on a satellite system.

Keywords: cyber, cybersecurity, cyber exercise, cyber threats, cyber governance, civilian use of space, critical infrastructure, military use of space, policy, regulations, standards, the satellite industry, the space industry

This thesis is written in English and is 69 pages long, including 5 chapters, 12 figures, 3 tables and 4 appendixes.

List of abbreviations

C2	Command and Control
CCDCOE	Cooperative Cyber Defence Center of Excellence
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Critical Infrastructure Sector
GNSS	Global Navigation Satellite System
COMSATCOM	Commercial Satellite Communication
CRSRA	Commercial Remote Sensing Regulatory Affairs
CSCO	Commercial Satellite Communications Office
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOT	Department of Transportation
EW	Electronic Warfare
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
GAO	Government Accountability Office
GDPR	General Data Protection Regulation
GEO	Geostationary Earth Orbit
HEO	Highly Elliptical orbit
GPS	Global Positioning System
IA-PRE	Infrastructure Asset Pre-Assessment Program
ITU	International Telecommunication Union
INMARSAT	International Maritime Satellites
InSAR	Interferometric Synthetic-Aperture Radar
IMT	International Mobile Communication
ISAC	Information Sharing and Analysis Center
ISR	Intelligence, Surveillance, and Reconnaissance
LEO	Low Earth Orbit

MARFORSPACE	Marine Corps Forces Space Command
MEO	Medium Earth Orbit
MILSATCOM	Military Satellite Communication
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAVSPACE	Navy Space Command
NESDIS	National Environmental Satellite, Data, and Information Service
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NROL	National Reconnaissance Office Launch
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
RFP	Request for Proposals
SATCOM	Satellite Communication
SME	Small and Medium-sized Enterprise
PNT	Positioning, Navigation, and Timing
UNOOSA	United Nations Office for Outer Space Affairs
USASMDC	United States Army Space and Missile Defense Command
USSF	United States Space Force
USCENTCOM	United States Central Command

Table of Contents

List of Figures

List of Tables

1 Introduction

The late 1950s marked the beginning of the space race. The Soviet Union launched the first artificial Earth satellite "Sputnik 1" on October 4, 1957 [1]. It took the United States over four months to successfully launch Explorer 1. American first artificial satellite was launched on January 31, 1958[2].

Since 1957 the number of satellites, their capacity, and functionality significantly increased. According to the United Nations Office for Outer Space Affairs (UNOOSA) in April 2022, about 8,554 satellites are orbiting the Earth. About 1,745 satellites were launched in 2021[3]. From purely defense capabilities, the commercialization of the satellite market spread to every aspect of our daily lives. Societies use satellite-based services for mobile communication, the internet, a variety of IoT devices, etc.

Space activities were once under full government control. Governments were financing, designing, engineering, manufacturing, launching, and operating satellites single-handedly. The first *commercial* satellite launch took place in 1989 in the United States[4]. Since 1989, over 450 commercial satellite launches were conducted[5].

A little over a decade later the "New Space" economy started to take shape. Companies and entrepreneurs began to acquire equity funding to develop space projects independently, without government involvement. A large part of the New Space economy comprises satellites, small satellites, and microlaunchers[6]. Figure 1 illustrates the rate of growth of commercial companies involved in space and satellite development.

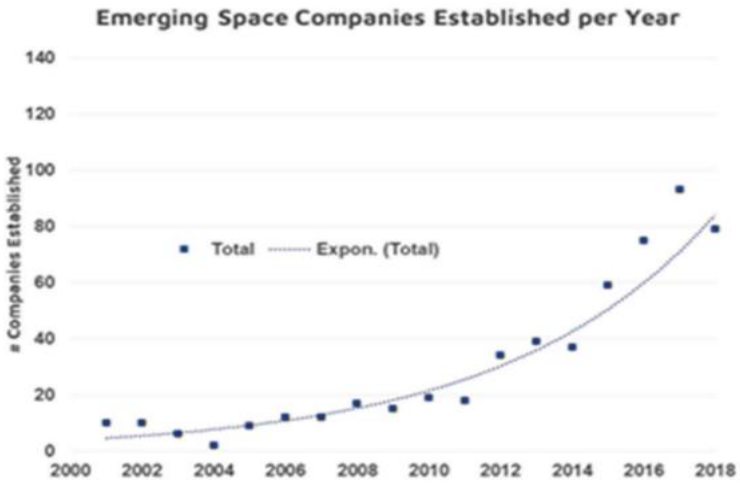

Figure 2: Growth of New Space Companies
Source: Adapted from [6] [1]

[1] The Figure is taken from [6], with the original source identified as NSR, Emerging Market Analysis, 2nd edition (NSR, Cambridge MA, 2019).

For the near future, SpaceX announced its plans to launch additional 4,425 Starlink satellites and Boeing plans to put an extra 2956 satellites in orbit, for the internet-from-space mega constellations[7].

The space industry is expanding, and the U.S. government is one of its main customers. The global space market is growing as well. In 2021 the space market was valued at US$388.50 billion. It is predicted to reach US$540.75 billion by 2026[8].

The cybersecurity concern for satellites and space assets is not the U.S. specific. It applies to the majority of countries that base their critical services on satellite data.

1.1 Problem Statement

Cybersecurity governance of the satellite industry is a complex issue that is quickly becoming a prominent concern in the tech and space industry, as well as among policymakers on national, regional, and international levels[9][10][11]. Cyber threats and vulnerabilities to satellite systems are mission-critical and would lead to disastrous economic, political, and geostrategic consequences[10]. The complexity of the issue also stems from competing priorities during IT systems development, the exponential growth of space and satellite industry sectors, and the arrival of multiple private actors with different levels of cyber awareness[11]. Additionally, there is no internationally recognized governance structure that can become a reliable foundation. According to Housen-Couriel [9], a dedicated cooperation framework is in high demand in order to counter rapidly developing cyber-enabled threats to satellite systems.

The disturbance of any segment of the satellite system either the ground station, link segment, or space segment poses a dire strategic risk to satellite dependent critical infrastructure including the financial system, electric grid, Global Navigation Satellite System (GNSS), and military capabilities[12],[13], [14]. According to Garino [12], tracking or monitoring satellite transmission can enhance adversary force intelligence preparedness. Consecutively, satellite operators need to include threat actor profiles in their risk assessments and tolerance, including challenges to cybersecurity in space from state and non-state actors[14].

Although a number of factors have been suggested as a threat to satellites, it is important to understand that many of the challenges can be addressed through exercising principles of cybersecurity governance, understanding the risks, training the audience for the most likely

scenario, and considering the impact of the human factor as well as the value of strategic coordination[15][16][17].

Unfortunately, due to novelty and complexity, very little attention has been given in the literature to the holistic discussion of ways to improve the overall approach to satellite cybersecurity and governance issues.

As indicated, the topic of the study is the satellite industry. The literature review helped to establish the research problem of the thesis. The research problem is the inadequate state of cybersecurity governance in the highly interconnected satellite sector.

Ellis and Levy [18] define two conditions that must be present for a "research-worthy problem" to exist. The first condition is that "the current state differs from the ideal state". This condition is met as the state of cybersecurity governance in the satellite industry is troublesome and far from the desired state. It is made clear by the bipartisan support for several draft legislation that precisely addresses the cybersecurity of satellites in the United States. Chapter 3 in detail construes this issue and adds other evidence to the statement that the space industry needs better cyber management.

The second condition for the research worthy problem is the absence of "an "acceptable" solution available"[18]. Literature on the satellite industry and cybersecurity for space focuses mostly on technical solutions. In the past, almost every satellite system was unique and required individual IT solutions. Nowadays with more satellite operators using commercial-off-the-shelf software solutions, the cyber risks to systems and missions are increasingly high. It requires overall cyber policy evolvement and tailoring to the satellite industry rather than the availability of only technical solutions. There is no adequate solution or substantial discussion on how to strengthen cybersecurity governance in the satellite industry yet available.

The goal of the research is to produce a descriptive case study and develop integrated yet specific policy recommendations for strengthening cybersecurity cooperation in the commercial satellite industry.

1.2 Research Questions and Objectives

The overarching research objective of the thesis is to develop an understanding of how to improve the cybersecurity posture of the satellite industry in the United States. The thesis aims to examine the challenges that the satellite industry faces in terms of cybersecurity

guidance, policies, and regulations. The research assesses current threats to the industry and space assets in the United States. However, due to the global nature of the industry, the threats to space systems are not U.S. specific and apply to European countries as well. The thesis analyzes then analyzes the threats and regulation gaps through the lens of cyber exercises to determine the potential impact.

The specific research objectives (RO) of the thesis are:

RO1: To develop integrated policy recommendations for strengthening cybersecurity in the U.S. satellite industry.

RO2: To identify existing cybersecurity regulations for satellites, including roles and responsibilities during incident response.

RO3: To develop a comprehensive description of major cyber threats to satellite systems.

RO4: To determine the impact of cyber exercises "lessons learned" on informing policy decision making.

Building upon the research gap and research objectives, the main research question (RQ) is formulated.

Main RQ: How to improve cybersecurity governance of the satellite industry?

There are three additional research questions that feed into the main RQ.

RQ1: How is cyber security addressed on strategic and policy levels in the United States.

The research question investigates the landscape and availability of strategic and policy frameworks in order to identify available gaps. Once gaps are identified, it allows to tailor policy recommendations to a more specific area.

RQ2: What are the main threats and vulnerabilities of satellite systems?

This research question allows for a holistic assessment of known threats, vulnerabilities, and threat actors in order to understand if they are any different from a regular cyber threat. If space threats are different, then alternative defense approaches should be deployed. If the cyber threats to satellite systems mirror cyber threats to Earth networks, then similar approaches could be deployed.

RQ3: How can cyber exercises contribute to cybersecurity policy development for satellite systems?

The question considers existing cyber exercises and evaluates their effectiveness in identifying bottlenecks and developing recommendations for better cyber defense and resilience.

1.3 Theoretical Approach

Cybersecurity is no longer an obscure term only IT professionals understand. From a purely technical subject, cybersecurity became a political and global consideration for nation-states, international organizations, private companies, and non-state actors. Cybersecurity affects most aspects of our lives. Bad cyber hygiene can allow criminals to steal money from an individual bank account. Offensive cybersecurity operations can penetrate the world's most secure networks or interfere in national elections.

Cybersecurity is a complex field. Even understanding the level of analysis of cyberspace is a complicated issue. What is being defended: the state, the critical infrastructure, commercial companies, or an individual?

Joseph Nye's dissection of cyberspace complexity and layering is an effective way to frame the discussion for political analysis and theoretical scrutiny of the cyber domain. According to Nye[19], the "cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional "commons." It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult. Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer"[19].

Combining the man-made nature of the cyber environment and the global reach of the field, the complex theoretical approach provides the most fitting theoretical framework to merge cybersecurity and space assets. Satellite systems are complex interconnected networks. The complex theoretical approach allows understanding the foundational need for stronger cyber policies and cooperation in the space industry.

Often, cybersecurity concerns are analyzed through a technical lens. However, it is vital to apply a comprehensive approach to successfully improve and strengthen the cybersecurity posture of an organization or a nation-state. A combination of Systems and Complexity Leadership theories as proposed by Susan M. Tisdale provide a strong theoretical background to discuss cybersecurity policies for complex, interconnected satellite systems as well as support the significance of cyber exercises in informing policy for the commercial satellite industry.

Tisdale[20], provides an excellent summary of the Systems theory as described in Skyttner's 2006 book "General Systems Theory: Problems, Perspectives, Practice". According to Tisdale's analysis, the theory has the following characteristics that also include "(1) interaction between systems to achieve goals; (2) transforming systems to achieve the goal; (3) environmental and other disorderly factors on systems; (4) regulatory impact on systems; (5) system hierarchies and subsystems impact on the system; (6) differentiation among the subsystems; and (7) multiple/alternative ways to achieve system objectives[20]."

Complexity Leadership Theory "addresses the dynamic interactions in a global economy where organizations and management styles need to adapt quickly to meet new challenges" [20].

The Systems and Complexity theory "argues that issues should be addressed from all aspects of an organization and at all levels"[20]. That is in line with the holistic research approach of this thesis.

The thesis consists of five chapters. The introductory *Chapter 1* defined the problem and provided an outline of the research questions and objectives.

Chapter 2 presents an extensive literature review focusing on a high-level description of the existing cyber policy in the U.S., general use of satellites by the U.S, definition of specific cybersecurity risks in space, and evaluation of analytical writings on the theory of wargaming and impact of cyber exercises.

Chapter 3 discusses the case in detail. It describes specific policies and regulations on the subject of satellite cybersecurity in the United States, outlines the military and civilian use of satellite capabilities, discusses specific cyber-attacks on satellites, and describes existing cyber exercises. The chapter also provides an in-depth research methodology description, data collection, and analysis methods.

Chapter 4 presents the result and discussion based on the interviews, the survey, and the literature review. It also objectively defines the limitations of this research.

Chapter 5 provides actionable policy recommendations based on the comprehensive data collection processes. The chapter also summarizes the whole thesis and points out research problems for future exploration.

2 Literature Review

The literature review chapter has the goal to summarize state-of-the-art knowledge in the field of cybersecurity policy for the satellite industry in the United States and identify gaps for further examination. Scholarly research is not widely available on the nexus of cyber and space policy due to the novelty of the subject and the only recent increase of attention of policymakers to this matter. The literature review revealed that sources from the government, private sector, and research institutions prevail in number and relevance over purely academic books and articles.

The analysis of any space-based capabilities is a delicate issue due to its dual-use nature. The thesis focuses on commercial application, yet the military continuously relies on and contacts the private sector for space missions. While the best effort is taken to concentrate on commercial and civilian use, it is inevitable to incorporate military resources and approaches to create an in-depth depiction of the field. During the literature review, several reoccurring themes were identified.

The discussion of cybersecurity for the commercial satellite industry is still in its early stages. The debate over approaches, rules, and regulations has intensified in the past couple of years both in the United States and Europe.

The need for a new space cybersecurity regime. The International Security Department of Chatham House conducted multi-year, interdisciplinary research on cybersecurity and space security. The project in detail identified specific threats and ways how cybersecurity attacks can be used against satellites to destroy or impede their function. The research was conducted by partnering with cyber, space, and policy experts from different counties and international organizations to solicit their views on the problem of cybersecurity and space. There were also several roundtables with industry professionals discussing existing issues. Among other recommendations, the project concluded in 2016 with a recommendation to create an international space cybersecurity regime and design recommendations for its functions[21][22].

Many satellite systems suffer from poor cybersecurity. U.S. Department of Defense has experienced unfavorable cybersecurity assessments of some of its critical systems. The ultra-high frequency (narrowband) military satellite communications system, the Mobile User Objective System (MUOS) had cyber issues in 2015 and 2019. During operational testing, it was found that MUOS satellites and ground systems were not operating securely due to the ground systems having proven security concerns[23]. NASA has been struggling with a bad

cybersecurity stance for many years. The recent report by the Office of Inspector General found that due to decentralized cybersecurity approaches and ad-hoc investments in IT, NASA is at a higher-than-necessary risk from cyber threats[24].

Cyber security threats to space assets used to be largely ignored, yet the approaches are changing. Security of satellites and space assets has always been important. In the past, the threat of anti-satellite missiles was a major consideration [25], [26]. With the rapid development of digital weapons, the threat profile of satellite security is now dominated by cybersecurity considerations. The U.S. Space Development Agency "looked at potential threats to its satellites and is less worried about missile strikes than it is about cyber-attacks and intrusions into the supply chain[27]".

Most of the world's critical infrastructure daily relies on space-based assets. Industries such as communication, maritime trade, air transport, financial services, weather monitoring, and national defense – all heavily rely on secure space infrastructure. Such dependence creates severe but often unrecognized security threats [28], [29].

2.1 U.S. Cyber Policy

There are many standards, policies, strategies, and regulations that generally address cybersecurity or the space sectors. This research aims to map out existing legal and policy guidance that narrowly applies to the cybersecurity of satellites in the U.S. It explores how and on what regulatory level cybersecurity is discussed and how satellite services are used by the U.S. Government.

In 2010 Title 51 was added to the United States Code titled National and Commercial Space Programs Act (NCSPA). The purpose of the Act was "to codify certain existing laws related to national and commercial space programs as a positive law title of the United States Code[29]". The positive law did not introduce any new legislation but streamlined and organized existing legislation and eliminated contradictions in existing law. Among other subjects, the Act addresses licensing issue for satellites and other space crafts and discuss security applications of space systems for America. Notably, cybersecurity considerations were missing. Even though the commercialization of space was already viewed as a crucial part of the American future, protecting the assets from cyber threats was not even an area of discussion at that point in time.

Currently, many more government core functions depend on stable and secure communication means. The rapid development of the satellite industry made it an attractive

target for cyber-attacks. The industry and technology grew faster than the government's ability to address emerging threats on the legislative and regulation side. Diversification of providers of satellite services and the impact on national critical infrastructure made the U.S. government aware of the potential cyber threat the industry could face if continues to be unregulated and unsupported.

2.2. Use of Satellites by the U.S. Government

Space and satellite technology are dual-use in nature[30]. The applicability of technology to both, defense and civilian industries highlight multiple interdependencies and the scope of impact in case of cyber compromise. It builds the case to assign a higher value to the cybersecurity requirements of commercial satellites. In general, there are four main uses of satellites. Table 1 presents the overview of the satellite missions and their application for military and civilian use. This is a good representation of the dual-use capability of each satellite. The data in the table is adapted from the 2019 and 2022 reports by the U.S. Defense Intelligence Agency on the Challenges to Security in Space.

Table 1. Overview of Main Satellite Missions for Military and Civilian Use.

Source: Adapted from [14], [31]

<table>
<tr><th>Type of satellite mission</th><th>Military application</th><th>Civilian application</th></tr>
<tr><td rowspan="2">Position Navigation and Timing - PNT</td><td colspan="2">• Timing signals for applications in air, land, sea, and space navigation.
• GNSS and GPS - provide position and navigation data for directions for routine activities.</td></tr>
<tr><td>• Precision weapons guidance.
• Assets tracking.</td><td>• Aviation and drones.
• Planning more efficient routes and managing route congestion.
• Autonomous vehicle guidance.
• Precision farming.
• Banking transactions.
• Synchronization for electrical power grid.
• Emergency medical, fire and police services.</td></tr>
<tr><td rowspan="2">Communications</td><td colspan="2">Used for beyond-line of-sight communications. Support global communications and complement terrestrial communications networks.</td></tr>
<tr><td>• Improve situational awareness.
• Greater mobility of forces.
• Eliminates the need for ground-based infrastructure.</td><td>• TV, phones, internet, all communication means.</td></tr>
</table>

Remote Sensing or ISR (Intelligence Surveillance and Reconnaissance)	Provides data on the Earth's land, sea, atmosphere, terrain, environment, and crisis management	
	• Provides ISR data. • Identify adversary capabilities • Track troop movements and locate potential targets. • Observe related events and locations.	• Weather forecasting. • Preparing for weather emergencies. • Assisting businesses in determining areas with mineral resources. • Assisting farmers in identifying potential agricultural disasters. • Insurance. • Monitoring Infrastructure.
Science and Exploration	• Technological innovation. • Insights into the nature of Earth and the Universe. • Technological advances such as cell phone cameras, better metal alloys for jet engine turbines, solar panels, memory foam, portable computers, compact water purification systems.	

2.3 Cybersecurity Risks in Space

There are several types of orbits used for satellites. The four most common orbit types are Geostationary Earth Orbit (GEO), highly elliptical orbit (HEO), medium Earth orbit (MEO), and Low Earth Orbit (LEO)[32]. European Space agency also distinguishes Polar orbit and Sun-synchronous orbit (SSO), which is a type of LEO, Transfer orbits, geostationary transfer orbit (GTO,) and Lagrange points (L-points)[33]. Figure 2 demonstrates the main Earth orbits.

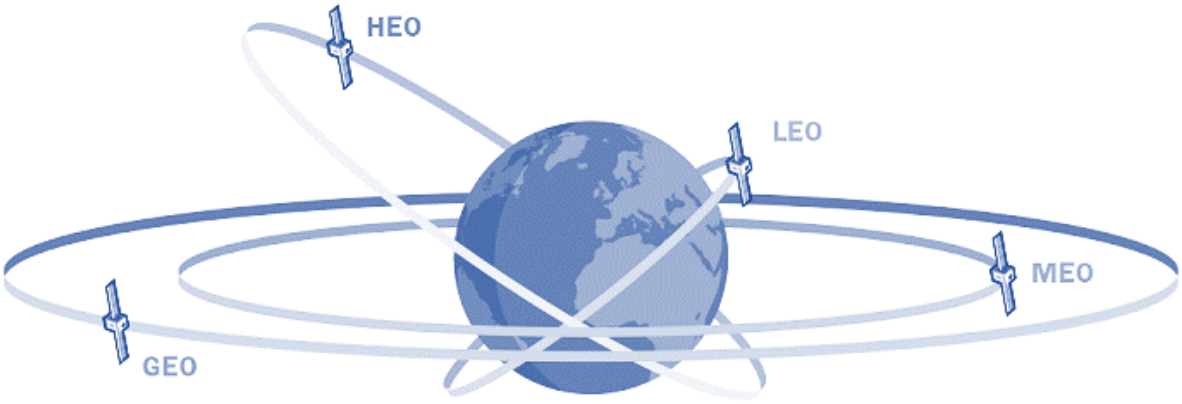

Figure 2: Earth Main Orbits

Source: Adapted from [34]

Each orbit has its characteristics and is best suited for certain types of satellite missions. Also, each orbit has its risks, vulnerabilities, and advantages. Table 2 describes each orbit,

highlights the best applications, and points out some high-level vulnerabilities. The table is based on the data from the European Space Agency and table from the Joint Publication of the U.S. Department of the Navy and the U.S. Department of the Army on Space Operations.

Table 2. Orbit Types, Advantages and Vulnerabilities. Source: Adapted from [32], [33]

Orbit	Description	Advantages	Vulnerabilities	Civilian and Military Applications
GEO Geosynchronous Earth orbit	• Roughly circular • ~37 km (23,000 mi) above Earth's surface • 'Stationary' over a fixed position	• Continuous coverage over specific area • Coverage nearly hemispheric • Cover large range of Earth, as few as three equally spaced satellites can provide near global coverage	• Far from Earth - resolution and signal limitations • Easier to jam signal latency	• Telecommunication • Surveillance • Reconnaissance • Weather collection • Missile warning
HEO Highly elliptical orbit	• Long ellipse • ~965-40,000 km (~600 - 25,000 mi) perigee/apogee	• Long dwell time over a large area • Coverage of high North or South latitudes	• Continuous coverage requires multiple satellites	• Communication over high North or South latitudes • Scientific surveillance • Reconnaissance • Missile warning
MEO Medium Earth orbit	No need for specific path around Earth • Roughly circular • Between ~1,600-35,000km (~1,000-22,000 mi) above Earth's surface	• Stable orbit • Less signal latency	• Highest radiation level environment	• GNSS/GPS • PNT • Communication • Tracking large jumbo jets • Getting directions to a smartphone
LEO Low Earth orbit	No need for specific path around Earth • Roughly circular • As high as ~1,600 km (~1,000 mi) above Earth's surface • As low as 160 km (100 mi) above Earth	• High resolution images • High signal strength • International Space Station (ISS) is on this orbit	• Best for large satellite constellations • Single satellite is less useful for communications due to velocity • Small coverage area over Earth surface • Limited coverage windows for any specific geographic region	• Internet • Surveillance • Reconnaissance • Weather collection • Manned space flight • Communications

2.3.1 Cybersecurity Risks to Satellites

The literature identifies several different segments of a satellite. For the purpose of this research, the simplest depiction of the architecture is used. There are three main segments that make up any satellite system: the space segment, link segment, and ground segment[31], [35]. All segments of the architecture are vulnerable to a cyber-attack. Naturally, all segments are also vulnerable to physical and electronic attacks. Any type of attack can disrupt, break down or compromise a connection between the ground segment and space segment[31].

The schema of the system is presented in Figure 3.

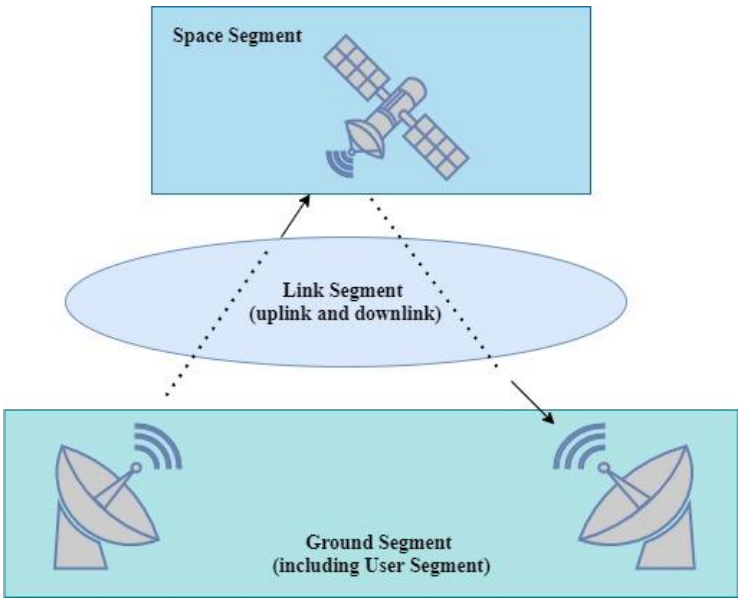

Figure 3: Simple Satellite System Architecture

Source: Designed by the author

The satellite cyber-attacks can be divided into three main groups[36]:

1. **Data Intercept or Monitoring.** Jamming and Eavesdropping modes of attack are used for data interception and monitoring attacks.

   Jamming – is considered the easiest form of satellite hacking. However, sometimes it can fall under electronic warfare (EW), rather than cyber but it depends on the means[37]. According to the manufacturer of jamming equipment "Phantom Technologies", there are two ways to jam a satellite. "First is to target the uplink, the transmissions coming from the ground to the satellite. This can be done by generating a jamming signal in the same specific frequency and aiming it at the satellite, so the satellite cannot distinguish between the actual communication and the noise. The second option is to disrupt the downlink, the transmissions from the satellite to the ground forces. [..] the satellite jammer generates noise in the target

frequency, however in this case, instead of aiming the signal at the satellite, the jamming unit will emit signals that cover a surface area in which [user] will be waiting to receive communications. The transmitting power that is required to 'confuse' the satellite is quite high, however, once achieved, it effectively jams the satellite for all ground communications. Jamming the downlink requires much less power, but its effect is limited accordingly, both in distance and to receiving terminal antennas that have a line of sight to the jammer. Size and transmission power will determine the jamming range (downlink satellite jammers can be minimized to the size of a handheld jammer)[38] ."

Eavesdropping is when access to satellite telecommunication (TV, Internet, phone) is obtained without the distraction or manipulation of the data. This mode "monitors" the satellite data. This type of attack receives very little attention, therefore is an appealing vector for further development and research[37]. The data intercept/monitoring attack is reversible[36].

2. **Data corruption.** Hijacking and spoofing are the prominent modes for the data corruption attack. *Hijacking* is "illegally using a satellite to transmit the hackers signal, in some cases overriding legitimate traffic[37]". The biggest concern of this type of attack is data manipulation. Data integrity is vital for military or civilian applications. *Spoofing* is "the ability to capture, alter, and retransmit a communication stream in a way that misleads the recipient[12]." The data corruption type of attacks are usually reversible[36].
3. **Seizure of Control.** It is a type of cyber-attack that compromises telemetry, tracking, and command (TT&C) communication links. This attack can "make" the satellite exhaust all of its power, prematurely re-enter Earth's atmosphere, rotate the antennas and solar panels in an opposite direction, etc. Such an attack can turn a satellite into a brick or an assault weapon against other space assets. This is one of the most complicated types of attack on a satellite[37]. This may be an irreversible attack[36].

Ground Segment. The main function of the ground station is to communicate with the satellite. The ground station uses antennas to do so. Majority of the satellites, both military and civilian use ground stations for command, control, and management of satellite operations. The ground stations are in continuous operational mode 365 days a year[13]. As the ground station

represents a physical terrestrial object, it is the easiest segment to attack. If successful, it allows for a straightforward way to control and track a satellite[11].

Link Segment or Communication Segment. The segment connects the ground segment with the space segment through the links that are identified as control or mission links. Control links transmit commands to the satellite and its sensors. Mission links interpret the operational data sent to or from the satellite. These links are vulnerable to multiple types of cyber and electronic attacks like jamming and spoofing[12].

Space Segment. Satellites are complex, expensive, and somewhat fragile constructions. That makes them vulnerable to multiple lethal attacks, including kinetic energy and directed energy (laser and high-powered RF) [12]. Vulnerabilities in ground stations, network components, and the receivers which acquire data from the satellite are the root causes of most cyber threats to the space segment. Such vulnerabilities allow attackers to breach the network and remain undetected. Supply chain attack is another vector for space segment as malicious software can be introduced with the hardware to cause damage in the future[39].

In addition to data manipulation and seizure of control attacks, there are other examples of specific attacks relevant to all three satellite segments[11]:

- **Physical attacks.** Compromising physical security measures, such as gaining unauthorized access to a ground station and other physical IT assets. A successful attack can disable the ground station or overtake control of the satellite system without compromising the communication links of the space system. Loss of Command and Control functionality can happen in other ways as well.
- **Computer network exploitation (CNE) attack.** In this case, an attacker is targeting a network to which a ground station is connected. Such attacks can happen through usual means such as poor system configuration, unauthorized access, or phishing.
- **Failure of the cloud infrastructure**. Cloud services power the majority of the current ground station can lead to catastrophic consequences and compromise operations of critical real-time satellite systems.
- **Data corruption,** intentional or non-intentional data modification. This can lead to hardware failure, active attempts to deny data use, software failures, etc.

- **Supply chain attacks** such as software leaks, open-source investigations, and common component use. This creates vulnerabilities and exploits that are integrated into the supply chain.

    - **Unpatched software**. Legacy or outdated commercial-off-the-shelf software is a known attack vector. It allows for use of known vulnerabilities to overtake command and control systems.

Another underlying risk to the cybersecurity of satellites is the availability and use of Commercial off-the-shelf (COTS) software and hardware solutions. The technologies used by large satellites and small satellites are not so much different. COTS devices are fast to adopt new technologies to achieve “rapid product cycles with high utility at low cost, combined with a more agile management and business style” [7]. The agile cycle of adoption and production without appropriate cybersecurity compliance procedures is one of the weakest links in the space supply chain and must be addressed holistically on the level of technical requirements as well as managerial coordination.

2.3.3 Threat Actors

The majority of the U.S. military capabilities and civilian communication depend on satellite systems which makes the United States the most vulnerable to space attacks[12]. “We simply cannot afford to defend against all possible threats. We must know accurately where the threat is coming from and concentrate our resources in that direction" said Edwin Land, the father of U.S. satellite reconnaissance[40].

The U.S. Defense Intelligence Agency identifies two usual suspects as the main threats to space systems: China and Russia. The report also describes Iran and North Kore as emerging challenges in the space domain. In three years between 2015 and 2018 China and Russia increased their satellite space systems by 200%. The following two years between 2019 and 2021 saw China and Russia grow their space capabilities by 70%[31].

China’s Cyberthreats in Space

The Chinese government views offensive cyberspace capabilities as a critical component of integrated warfare. China tailors its cyberwarfare capabilities to support military operations against space-based assets. One of the strategies is to establish information dominance in the early stages of conflict to constrain the adversary’s actions or slow deployment and movement of forces. Chinese army also undertakes cyber espionage against

foreign space entities in order to boost the level of technology and expertise available to support military research, development, and acquisition. Starting from 2007, there are confirmed cases of signal intelligence military unit participating in cyberespionage activities against U.S. and European satellite and aerospace industrial complex[31].

China continues to integrate "satellite reconnaissance and positioning, navigation, and timing—and satellite communications into its weapons and command-and-control systems to erode the U.S. military's information advantage.[41]"

Russia's Cyberthreats in Space

Russia's main strategy in cyberspace is the weaponization of information. Following the "Gerasimov doctrine" of 2013, cyber capabilities and information warfare became central to Russian defense strategy[42]. Russia views space-based data collecting and transmission as strategically important and has taken steps to improve its military's information offensive and defense units and capabilities[31].

Figure 4 illustrates the growth of Chinese and Russian satellites by mission type.

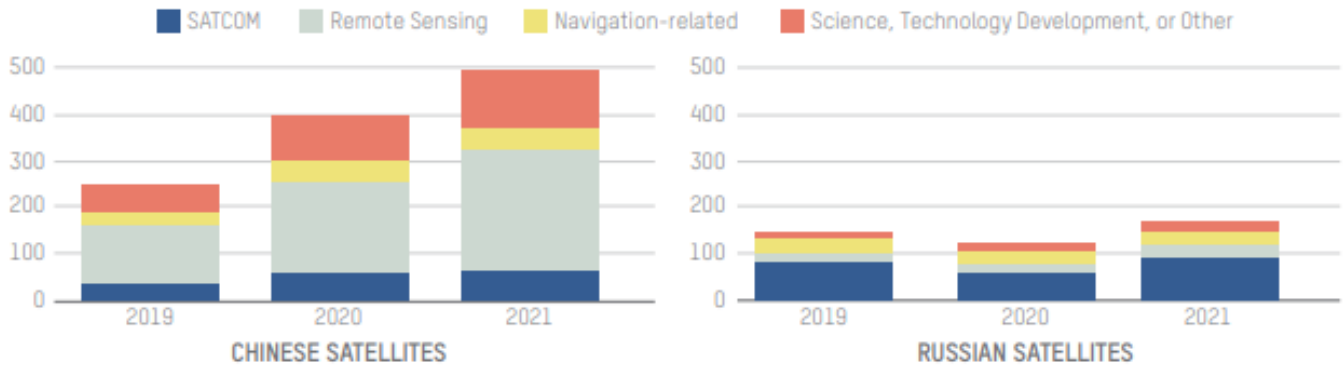

Figure 4: Growth of all Chinese and Russian Satellites, 2019-2021

Source: Adapted from [31]

The figure is indicative of China's offensive cyber strategy to increase its capabilities in remote sensing for better intelligence surveillance and reconnaissance. Russia's increase in SATCOM satellites is indicative of its strategy of weaponization of information and access to information.

Iran's Cyberthreats in Space

Iran has attempted to purchase Russian-made space-based intelligence surveillance and reconnaissance system since 2015. The system is still not in orbit. Russia would provide the

system and ground station support while Iran would operate the satellite. Iran's strategy consists of making every effort to prevent an adversary from using space during a confrontation. The government possesses a proven capability to disrupt space-based communications and GNSS signals. One of the state-owned companies has been actively promoting and selling GPS jammers on its website[31].

North Korea's Cyberthreats in Space

Another emerging challenge in the space domain is North Korea. It possesses similar cyber counter-space capabilities to jam GNSS/GPS and SATCOM and most likely preparing to deny space-based navigation and communications in the event of an armed conflict. The assumption is that North Korean state-sponsored hacking groups are probably targeting space technologies. It is important to anticipate and stop those attempts to hamper North Korea's ability to develop its space systems[31].

2.4 Cyber Exercises for Policy Planning

Cyber exercises take their root in traditional wargaming. There are different types of cyber wargames available. Each has its audience, objectives, and possible outcomes. The goal of any cyber exercise is to maximize learning about cybersecurity, coordination, and cyber policy issues. The participants are placed in an immersive environment within a wargaming system such as a cyber range. The ability to exercise in a controlled environment risk-free is aimed to provide clarity of the processes and effects[43].

Wilhelmson and Svensson [44] compare cyber exercises to crisis management exercises and stress the importance of training cooperation and communication during the exercise. The authors define the following contributions that cyber exercises make. Cyber exercises "

- Develop crisis management capabilities and leadership with responsible actors;
- Improve the ability to interact with other actors in the crisis management system;
- Increase the ability to make quick decisions and communicate situation information;
- Maintain awareness of the complexity that is characteristic of crisis situations.
- Examine and develop contingency plans that mirror reality.

- Point out areas where further training or [... exercise] are needed.
- Highlight weaknesses and strengths in resources and technology.
- Increase public awareness of the skills, capabilities, vulnerabilities, and needs.
- Develop the participants' ability and confidence in their competence.
- Enable those in the network the opportunity to know and understand each other better [44]."

The experience from a cyber exercise should not be replicable when the exercise runs again. If that occurs, it means that the design of the exercise is somewhat faulty, and participants are given too much restraint, which is not indicative of a real-life situation[43].

However, cyber exercises are not a substitution for traditional learning methods such as classes, workshops, and conferences. Cyber exercises allow to apply the learned concepts in a certain context [43].

Cyber exercise is "a way to experience the future without the risks attendant in the real world[45]" Cyber exercises are suitable tools for military, civilian, non-profit, and corporate leaders. It allows the leaders, managers, and executives "to test overarching strategies and specific plans before committing their organization, its people, and its resources to a course of action from which there is no turning back[45]."

Every wargame or cyber exercise generally follows similar phases of planning (Figure 5)

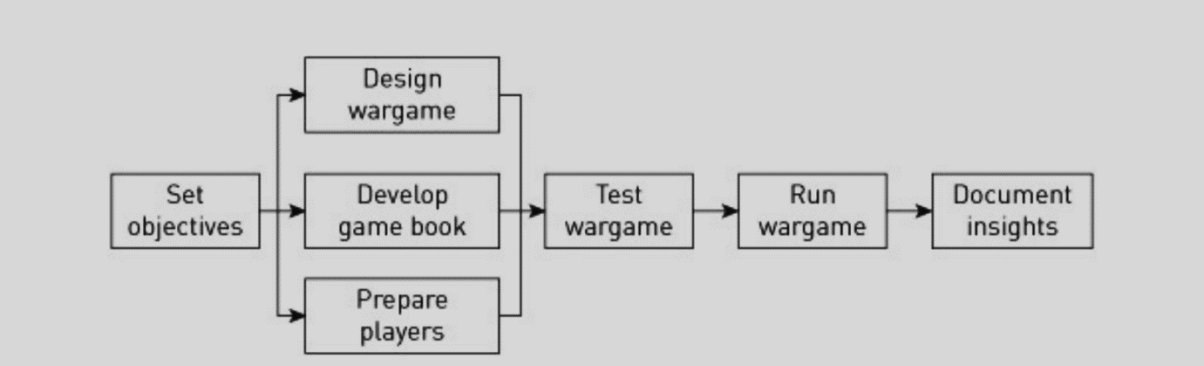

Figure 5: Phases of Exercise Planning

Source: Adapted from[45]

The goal of any cyber exercise is to train participants (and organizers as well) to exercise skills in several tracks [43]:

- Appropriate resource selection and tactical decision-making.

- Overcoming platform and system limitations.
- Rapid situational awareness.
- Delegating authority at the executive level.
- Assessing advice in a high-stress situation.
- Crisis leadership and strategic planning.
- Briefing subordinates.
- Implementing and modifying the plan as the situation changes.
- Evaluation and reevaluation of the plans and strategies.

Different types of cybersecurity exercises can target different audiences and goals, ranging from examining technical responses by critical infrastructure providers to evaluating diplomatic responses to a cyber incident. To fully comprehend the possibilities of cybersecurity exercises for policy work, it is necessary to define the different types and features of each cyber exercise [44].

Curry and Drage [43] define 4 types of cyber exercise. However, both classifications somewhat overlap and describe the same type of cyber exercise using a different title.

1. Penetration testing or red teaming.
2. BOGSAT (Bunch of Guys Sat Around a Table) Cyber wargames. Type of table-top exercise.

    2.1. "The train journey" – the game has a particular scenario, and pre-set events which will occur regardless of players' actions. The number of events is determined before the start of the game.

    2.2. "Choose your own adventure" – scenario has several options, presenting participants with several choices and not limiting with the "right" answer.

    2.3. "Active Opponent" – active red team that counters blue team moves live.
3. Interactive Cyber Wargames – when the players decisions and response has some measure of influence on the direction of future injects and outcomes of the game.
4. Analytical Cyber Wargames – designed for the purpose of analysis less than training.

Beigel and Schuetze [46] distinguish five types of cyber exercises:

1. Red Team/Blue Team Exercises.
2. Cyber Wargames.
3. Workshops.

4. Tabletop exercises.
5. Simulations.

According to Beigel and Schuetze [46], each type of exercise serves its specific purpose as shown in Figure 6.

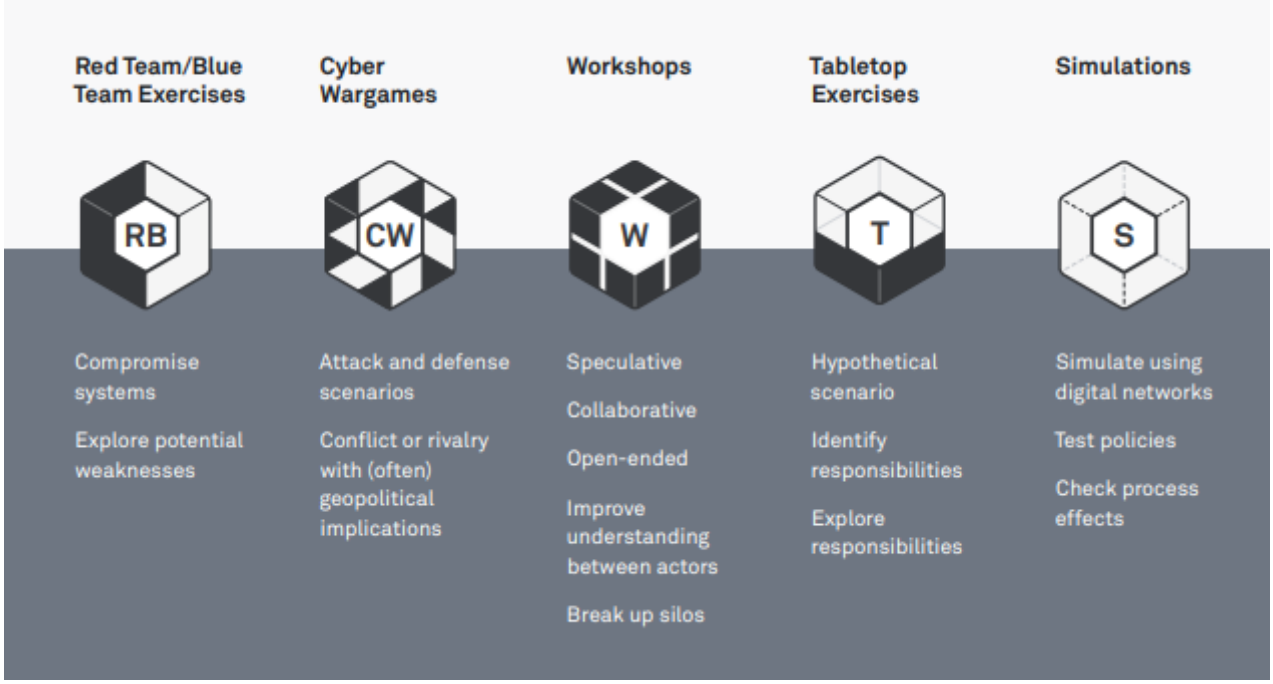

Figure 6: Defining Features of Cyber Exercise Types

Source: Adapted from [46]

When discussing cyber exercises for policy planning it is important to distinguish different stages of the policymaking process. In reality, stages overlap and are more complex, however, it is a good general framework. The five stages are **(1)** agenda setting, **(2)** policy formulation, **(3)** policy adoption, **(4)** policy implementation and administration, and **(5)** policy evaluation[47].

Beigel and Schuetze[46] consider the same five stages of the policymaking process and apply different types of cyber exercises to each step. The following table represents Beigel and Schuetze [46] assessment of different types of cyber exercises and their applicability to each policy planning stage.

Table 3. Relevance of Types of Cyber Exercises to the Policymaking Stages

Source: Adapted from [46]

	Type of Cyber Exercise

Policymaking stages	RT-BT	Cyber wargames	Workshops	Tabletop	Simulations
1. Agenda Setting	**Applies**	**Applies**	**Applies**	**No**	**No**
2. Formulation	**No**	**Applies**	**Applies**	**Applies**	**Applies**
3.Adoption	**No**	**Applies**	**No**	**Applies**	**No**
4.Implementation	**Applies**	**No**	**Applies**	**Applies**	**Applies**
5.Evaluation	**Applies**	**Applies**	**Applies**	**No**	**Applies**

3 The Case

Sputnik 1 was a simple satellite that could only communicate with the Earth through radio waves. Any radio amateur on Earth with the operational radio equipment using the correct frequency could catch Sputnik's signal. Those signals had the form of telegraph pulses[1]. Nowadays the architecture of satellites is much more complex. In essence, computing platforms are being launched into space with the ability to communicate with advanced ground stations or directly with the user equipment sometimes in real time[48].

The cheaper and easier access to space allowed more companies to offer their products and compete in the new lucrative market. The U.S. government also increased its reliance on the space and satellite industry. While space is not designated as one of the critical infrastructure sectors in the United States[49], dependency on satellite communication, navigation, and surveillance capabilities apply to most sectors. For example, the food and agriculture sector uses data from climate and weather observations satellites. The Department of Defense employs a variety of intelligence and communication satellites. Global Navigation Satellite System (GNSS) satellites are being used by the military and by the transportation industry. The majority of the critical infrastructure sectors heavily depend on global communications satellites[50].

3.1 Case Description

The U.S. government is increasing its efforts in protecting critical infrastructure from cyber-attacks. Cybersecurity and Infrastructure Security Agency (CISA) was created in 2018 with the mission to connect the "stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people"[51].

Despite the strong push to improve cyber resilience, there are disproportionately few efforts and mechanisms to improve cybersecurity for space systems.

Clear technical cybersecurity standards generally help with some of the concerns. There are many cybersecurity standards and frameworks that are used by the U.S. government. Some standards are mandatory, and some are created as guidance. While there are very few satellite-specific cybersecurity standards, the government should continue developing those space-specific frameworks. According to the survey on security framework adoption, the majority of the surveyed companies (84%) actively utilize a security framework. There is no single security

framework that is being used by the majority of companies, but each sector tends to have a prominent standard[52]. The space industry is technologically more complex than the majority of other critical sectors and is in need of more guidance, not less.

However, the availability of technical standards doesn't address the issue of cooperation and coordination. That is vital, especially for the interconnected satellite systems when the owner, operator, and consumer are often represented by different entities with different cultures, management, and understanding of cyber threats, incident response, and cyber resilience measures. The complexity of satellite systems requires designing tools best equipped to bridge the gap between technical capabilities and strategic planning.

3.1.1 National Level Strategies and Policy Directives

The United States government recognizes the importance of space and protecting space assets as the highest priorities for national security. The **National Security Strategy** of 2017[2] lists "advance space as a priority domain" and "promote space commerce" as priority actions for the space domain. On the side of cybersecurity, the Strategy calls to "improve attribution, accountability, and response", "enhance cyber tools and expertise" and "improve integration and agility" as priority actions [53]. The National Security Strategy was followed by the National Cyber Strategy in September 2018 and the National Space Policy in December 2020.

The **National Cyber Strategy** continued to stress the improvement of cybersecurity as a priority action. "Improve Space cybersecurity: The United States considers unfettered access to and freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. The Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure because these assets are critical to functions such as positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communications; and weather monitoring. The Administration will enhance efforts to protect our space assets and support infrastructure from evolving cyber threats, and we will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.[54]"

[2] As of April 2022, the United Strategy Government has not issued new National Security Strategy. There is an interim National Security Strategic Guidance issued in 2021 by the Biden Administration.

The **National Space Policy** further provides special guidelines on the cybersecurity of space systems. “In matters relating to cybersecurity for space systems the United States Government shall:

- Seek to ensure space systems and their supporting infrastructure, including software, are designed, developed, and operated using risk-based, cybersecurity-informed engineering;
- Collaborate with industry and encourage development and integration of cybersecurity plans for space systems that mitigate unauthorized access to critical space system functions, reduce vulnerabilities, protect ground systems, promote cybersecurity hygiene practices, and manage supply chain risks;
- Collaborate with interagency, allied, partner, and commercial space system operators to promote the development and adoption of best practices and mitigations;
- Leverage widely adopted best practices and standards in the creation of rules and regulations, as appropriate; and
- Determine appropriate cybersecurity measures for Government space systems through a mission risk assessment specific to a space system's design and operations[55].”

Policy Directives

National Strategies are not the only policy tools available to the White House. National Space Council is a part of the U.S. President’s Executive Office and is currently tasked with advising the President on space policy. In particular, the council is responsible to:

“(i) review, develop, and provide recommendations to the President on space policy and strategy;

(ii) coordinate the implementation of space policy and strategy;

(iii) synchronize the Nation’s civil, commercial, and national security space activities in furtherance of the objectives of the President’s national space policy and strategy;

(iv) facilitate resolution of differences among agencies on space-related policy and strategy matters;

(v) enable interagency cooperation, coordination, and information exchange on space activities; and

(vi) perform such other duties as the President may, from time to time, prescribe[56]."

In 2018, the Council authored a Space Policy Directive-3 (SPD-3), National Space Traffic Management Policy. The SPD-3 acknowledges the need for better security of satellites as "the need to establish satellite safety design guidelines and best practices" and "satellite and constellation owners should participate in a pre-launch certification process[57]." The SPD-3 paved the way for recognition of urgency for cybersecurity guidelines specific to satellites.

The three national level Strategies and SPD-3 create the necessary executive guidance for designing further policies. In line with the Strategies, the White House released the policy directive from the National Space Council "Cybersecurity Principles for Space Systems", known as SPD-5. The directive defines space systems as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A space system typically has three segments: a ground control network, a space vehicle, and a user or mission network. These systems include Government national security space systems, Government civil space systems, and private space systems[58]".

The policy lays out five broad principles for cybersecurity for satellites.

Space systems hardware, software, and supporting infrastructure should operate on a risk-based, cybersecurity-informed engineering.

Owners and operators of space systems should develop cybersecurity plans that would (a) protect against unauthorized access through effective authentication and encryption; (b) ensure physical protection of systems; (c) secure signal strength and monitoring throughout the mission lifecycle to prevent communication jamming and spoofing; (d) apply best practices of NIST Cybersecurity Framework to all segments of satellites, such as physical security, patching, logical of physical segregation, use of antivirus, staff training, etc.;(e) use intrusion detection and cybersecurity hygiene practices; (f) perform thorough supply chain risk management.

These principles should be implemented through rules, regulations, and guidance for managing space systems.

Cybersecurity threat information sharing should be improved as space system owners and operators are encouraged to better utilize Information Sharing and Analysis Centers capabilities or other similar platforms.

Cybersecurity measures should not be overbearing and interfere with mission goals. A certain level of appropriate risk tolerance is expected [58].

3.1.2 Federal Legislation and Policy Guidance

In January 2022, a bipartisan bill S.3511 known as the "Satellite Cybersecurity Act" was registered in the U.S. Senate – the upper chamber of the U.S. Congress. The bill is still in its introduction stage. It calls on Cybersecurity and Infrastructure Agency (CISA) to assist commercial satellite operators and develop a set of voluntary recommendations to protect satellite systems against cyber threats. Recommendations being voluntary is an unusual request, considering the importance of the matter. It also requests U.S. Government Accountability Office (GAO) to prepare a report on actions taken to support the cybersecurity of commercial satellites.

On March 30, 2022, the bill made it to the business meeting agenda of the Homeland Security and Government Affairs Committee of the Senate. It was "ordered to be reported with an amendment in the nature of a substitution favorably[59]." In practice, it means that a new updated version was introduced and will be treated as a draft for future considerations.

The substitute version increased the time for the report by the Controller General of the United States from 1 year to 2. The Bill does not ask for any funding at this point. The Report requested in the Bill is the right step toward consolidating available knowledge on U.S. Government dependence on satellites, mapping resources, and defining the gap in managing cybersecurity in the commercial satellite industry. The GAO Report should include information on the effectiveness of efforts of the U.S. Federal government, cybersecurity resources that are publicly available to the commercial satellites industry, and evaluation of coordination or duplication efforts among Federal agencies[60].

Two pieces of requested data stand out in the proposed Report. Congress wants to know "(3) the extent to which commercial satellite systems are reliant on or are relied on by critical infrastructure and an analysis of how commercial satellite systems, and the threats to such systems, are integrated into Federal and non-Federal critical infrastructure risk analyses and protection plans[60]" and "(4) the extent to which Federal agencies are reliant on commercial satellite systems and how Federal agencies mitigate cybersecurity risks associated with those systems[60]". This request is indicative of the gaps in the literature that fails to summarize and overarching meaning of satellites for the U.S Government operations across the board, not just by each agency.

This thesis was designed to describe the need for a well-rounded cyber policy and create an integrated approach toward considering U.S. reliance on commercial satellites.

The proposed Bill closely echoes the five principles describe in the Space Policy Directive-5 issued by the White House in 2020. Recommendations that are requested to be developed should be risk-based, plan for retention of control, protect against unauthorized access, jamming spoofing, physical security, management of supply chain, etc[57], [59], [60]. In some instances, the draft legislation borrows word-for-word the language from the Directive. It is significant in showcasing that the need for the new legislation has the support of the entire political spectrum and is based on the recommendations of the experts in space and cyber industries. The draft Bill has a long way before becoming a Law. It needs to pass through the Senate, and House, be submitted for President's signature, and only then become Law.

The non-regulatory Directives and the draft Bill are currently the only federal-level policy guidance specific to the cyber security of satellites. There are many cyber or space-specific policies and regulations available. Some of them overlap or complement each other. Satellite operators need to be aware of such overlaps and comply with all the regulations.

Policy Guidance

The role of the government in regulating the industry is not only about requirements and demands. Through regulation US government also provides knowledge and support in designing and managing space systems. The National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce is working on the internal report NISTIR 8270 "Introduction to Cybersecurity for Commercial Satellite Operations.[35]" The report is designed to support Directive SPD-5 and its goal to ensure secure access to and operations in space. The current second draft of the paper is still open to comments and suggestions by industry partners. Most of NIST's standards and recommendations are voluntary, yet impactful.

The target audience of the report is commercial satellite operators. The advisory value of this report for the industry and young startups is considerable. As a response to the SPD-5 Directive to support smaller businesses in the space industry, the NISTR 8270 provides a case study of cyber risk assessment for satellite operators.

The case study explains how the globally recognized NIST Cybersecurity Framework [61]applies to a low-Earth orbit small satellite vehicle. This is important as many companies, especially start-up satellite developers and operators do not prioritize cybersecurity. They want to get their products out fast and cheap, which usually means no budget for cybersecurity engineers or cyber risk managers on staff[62].

The case study applies Cybersecurity Framework Profile to the core cybersecurity areas of (1) Identify assets, (2) Protect assets, (3) Detect incidents (4) Respond to incidents, (5) Recover from incident. The scenario for the case study involves a small company that operates and manufactures commercial satellites and is focused on platform and payload. The case study demonstrates how each stage of the Cybersecurity Framework applies, mapping potential cybersecurity threats to business processes, building current profile of applicable subcategories, and referencing existing technical security and privacy controls (Risk Management Framework SP 800-53 [63]), provides risk assessment examples, and designs target profile. The most important part describes how to determine, analyze and prioritize gaps while comparing current and target profiles of the organization. The case study can be applied to different parts of space operations, but the principles and processes are well explained in this report[35].

3.1.3 Additional and Forthcoming Regulations

There are no specific cybersecurity regulations for satellites that would apply across the commercial satellite industry. Each agency has some sort of regulations, but they are not explicit for satellite cybersecurity. The relevant regulations usually cover the policy for communication encryption, operational security practices, network security, data security, privacy, etc. There are several federal agencies that will play a role in creating and maintaining cross-agency cooperation in satellite cybersecurity. The main agencies include but are not limited to the Department of Homeland Security, Department of Commerce, Department of Defense, the Federal Communications Commission, NASA, the National Executive Committee for Space-based Positioning, navigation and Timing and others [59].

The current landscape of cybersecurity regulations for satellites can be visualized like this:

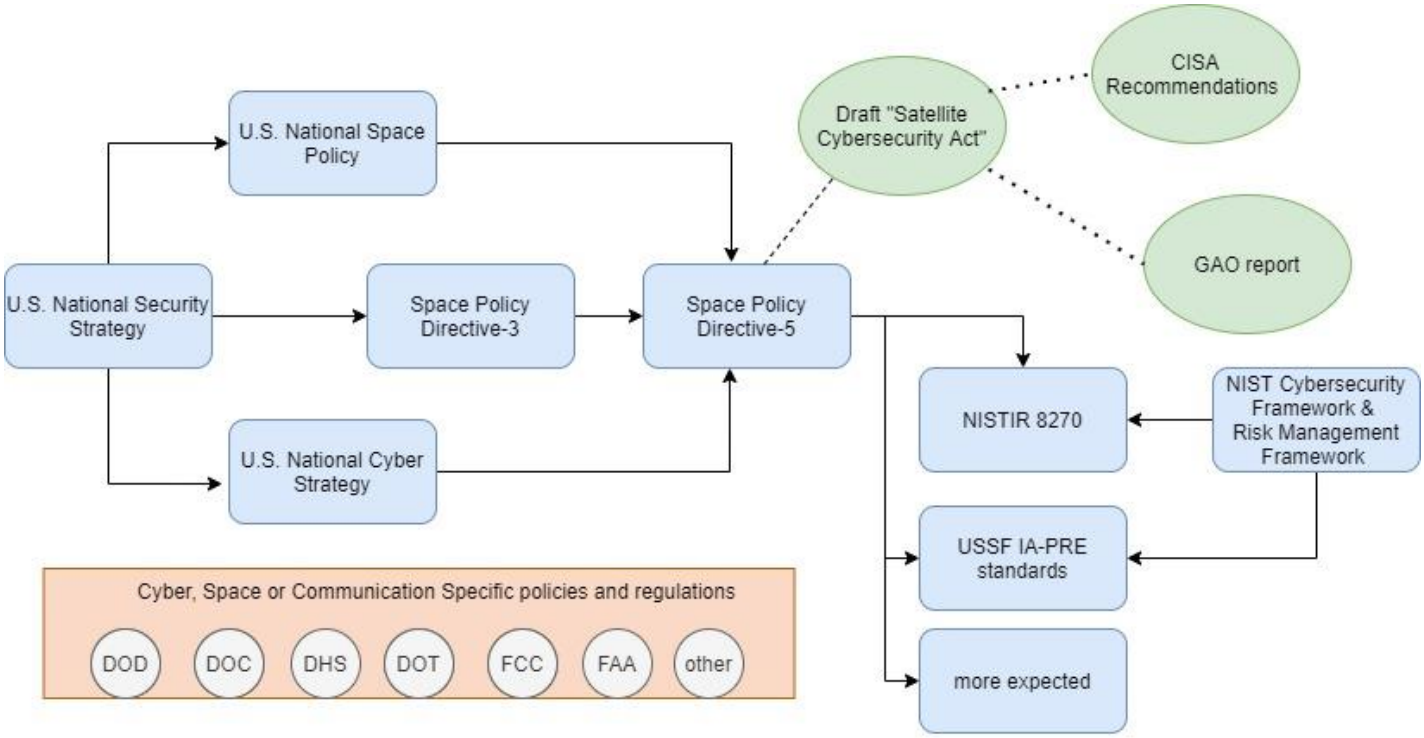

Figure7: Cybersecurity for Commercial Satellite Industry Regulatory Schema (non-classified)

Source: Author

In contrast, licensing of the commercial remote sensing industry has a much better developed and matured regulatory field. There are Laws, Regulations, Guidance, and Policies that address regulatory processes for remote sensing space systems and satellites [64].

Forthcoming Policy and Regulations

It is expected that soon U.S. Space Force will release a new classified strategy for integrating the commercial satellite industry into its operations [65]. The Strategy for the most part will be classified and Department of Defense specific, which puts it outside of the scope of this thesis. However, the need and reasoning behind designing this strategy apply to the whole spectrum of U.S. Government operations.

The head of SPACECOM at the USSF General Jim Dickinson explained that "Our relationship with a commercial industry is advancing, and developing and maturing very quickly[65]", and the integrated strategy is important because "we're finding that our commercial partners can bring a lot of capability very quickly to what we do each and every

day[65]", "the integration of commercial capabilities within US Space Command helps us with … providing resiliency, as well as redundancy in some of the things that we need and capabilities we provide[65]."

The U.S. Space Force Commercial Satellite Communications Office is also working on a highly anticipated and several times delayed Infrastructure Asset Pre-Assessment Program (IA-PRE). The goal of the IA-PRE Program is "to advance the security posture of current and future commercial satellite communications procurements for the Department of Defense. As the sole authority for procurement of COMSATCOM services for all of the DoD, the USSF must ensure the most secure space systems are available to support the U.S., its allies, and the joint warfighters[66]."

The long-delayed standards were supposed to be launched in 2020, then postponed to January 2022, with the plan to be fully in place by 2025[67]. However, there is a little public indication that the program is operational. Those standards are expected to be unclassified and can potentially serve as the industry's golden standard if found useful.

3.1.4 U.S. Military use of satellites

The research project conducted by the Colorado State University produced an aggregated table showcasing some of the U.S. defense satellites series with the description of their mission, purpose, and type. The table describes 220 out of 325+ assigned satellites[68]. According to the aggregated table, the main mission types and functionalities of military satellites are reconnaissance, military communication, and GNSS/GPS. Figure 8 shows the ratio of mission types. The data in real numbers is presented in Appendix 1 "Mission types in numbers".

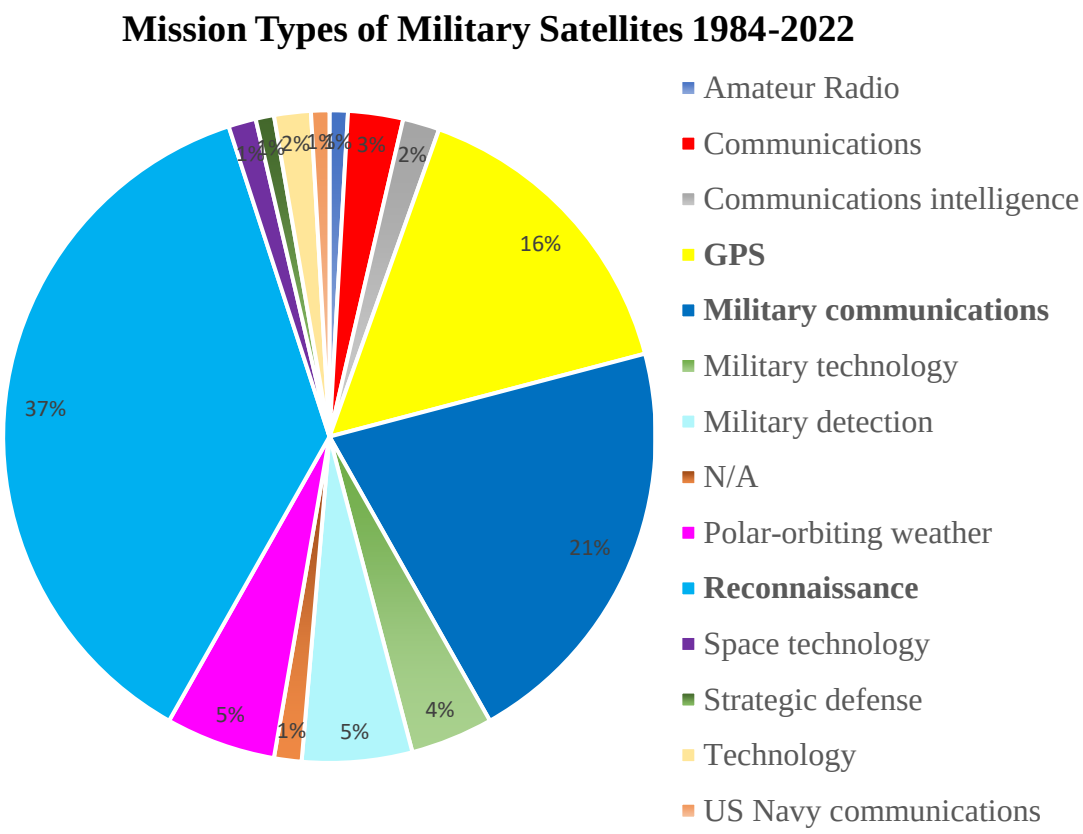

Figure 8: Mission Types of Military Satellites 1984-2022

Source: Data from [68], a figure created by the author

The role of commercial satellites in U.S. Government operations is critical to support national security priorities and contribute to economic growth. The Department of Defense spends billions of dollars a year on satellites for communication and other capabilities[69].

The Commercial Satellite Communications Office (CSCO) of the Space Force is the sole authority for the procurement of COMSATCOM services and capabilities for the DOD. In 2021-2023, the CSCO anticipates awarding around 3 billion USD in contracts to commercial entities in three service areas: (1) Transponded capacity, (2) Subscription services, and (3) End-to-end solutions[70].

It is important to understand what each service area means, as the Space Force is designed to play a more robust role in coordinating U.S. military engagements with space and commercial entities.

1. Transponded Capacity. COMSATCOM Transponded Capacity (CTC) “includes requirements with satellite bandwidth and power only, as well as limited

engineering services such as link budgets and transmission plans. It allows customer-proposed waveforms and industry-approved solutions to apply leased bandwidth to meet individual requirements.[70]".

2. Subscription Services. COMSATCOM Subscription Services (CSS) "are for use with fixed satellite services (FSS) or mobile satellite services (MSS). It uses contractor-determined waveforms that are billed on a per-use basis. CSS includes rates for vendor-defined network management monitoring engineering, integration, licensing, and operations required to deliver the services.[70]
3. End-to-end solution service area consists of Complex Commercial SATCOM Solutions and COMSATCOM Satellite Business Solutions.

Complex Commercial SATCOM Solutions (CS3) "allows DoD to build large, complex, custom satellite solutions. These include satellite transport (bandwidth), fixed or mobile satellite service, and service-enabling components such as terminals, handsets, and tail circuits with engineering services to integrate, operate, and maintain the solution[70]

COMSATCOM Satellite Business Solutions (SBS) is "a solution other than the FCSA solutions for FSS or MSS. Prospective acquisitions that are not anticipated to use FCSA solutions may utilize existing Blanket Purchase Agreements (BPAs), Indefinite-Delivery Indefinite-Quantity contracts (IDIQs), or using full and open competition[70]

The full list of projected awards is available in Appendix 2 "USSF CSCO Forecast to Industry"[70].

Multiple government agencies agree that contacting commercial satellites is cheaper and more secure than invest billions in the development of government-owned satellites. In July 2018 U.S. Government Accountability Office conducted a study of Military space systems and the use of commercial satellites to host defense payloads. The report concluded that DOD saves money and adds capabilities by procuring the resources of private companies for its satellite needs. By "using commercial satellites to host government sensors or communications packages—called payloads—may be one way DOD can achieve on-orbit capability faster and more affordably. Using hosted payloads may also help facilitate the proliferation of payloads in orbit, making it more difficult for an adversary to defeat a capability [69].

However, it is still challenging to have a comprehension description of involvement and integration of commercial capabilities into defense space infrastructure. The 2022 Appropriation Act for the Department of Defense under the Title VII – Reports and Others Matters request more clarity from the DoD on this issue. The Defense Department is required to produce a report of efforts to build integrated hybrid space architecture involving "the

Director of National Intelligence, in coordination with the Under Secretary of Defense for Intelligence and Security and the Director of the National Reconnaissance Office, shall submit to the appropriate congressional committees a report on the efforts of the intelligence community to build an integrated hybrid space architecture that combines national and commercial capabilities and large and small satellites[71].

Specifically, the Congress is interested in the analysis of how "the integrated hybrid space architecture approach is being realized in the overhead architecture of the National Reconnaissance Office[71]" and evaluation of "the benefits to the mission of the National Reconnaissance Office and the cost of integrating capabilities from smaller, proliferated satellites and data from commercial satellites with the national technical means architecture[71]." The hybrid space architecture improves the resilience and deterrence of space systems. It also distributes financial and cyber risks, allows to increase innovation pace, improves interoperability, and strengthens the U.S. space industry and U.S. space leadership[72].

Each branch of the Department of Defense has a dedicated Command for managing its satellite capabilities.

U.S. Army has a designated Space and Missile Defense Command (USASMDC). Within the Command there is a dedicated Satellite Operations Brigade that was created in 2019. The mission of the Brigade is to "executes continuous tactical, operational and strategic satellite communications payload management through its Wideband and Narrowband Consolidated SATCOM Systems Experts, Wideband SATCOM Operations Centers, Regional SATCOM Support Centers, and an Electromagnetic Interference mitigation detachment across the full spectrum of operations in support of combatant commands, services, U.S. government agencies, and international partners.[73]".

U.S. Navy structure is quite complex. It has Marine Corps Forces Space Command and Navy Space Command. Marine Forces Space Command (MARFORSPACE) is responsible to provide space operational support to the Marines. Navy Space Command (NavSpace) is responsible for cyber and space operations[74].

However, the Satellite Operational Brigade is scheduled to transition from Army to U.S. Space Force as USSF consolidates U.S. defense satellites under its umbrella. Space Delta 8 unit within the USSF is absorbing at least 11 of the Navy's narrowband communication satellites including the infrastructure[75].

3.1.5 U.S. Civilian Use of Satellites

In 2013, The Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21) was issued to "advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure[49]." The Directive defined 16 critical infrastructure sectors and corresponding responsible agencies. Space was not named as one of the critical infrastructure sectors. As the previous chapter on space regulation indicated, there are many agencies responsible for a narrow space industry segment. There is no single U.S. agency responsible for the resilience of the space industry or satellite sector. US Space Force is tasked with being a one-stop-shop for the military satellites, but it leaves the civilian part of the government uncoordinated. Designating space as a critical infrastructure sector would allow for a special agency responsible to maintain full awareness of threats and challenges as well as promote the development of the sector.

In June 2021, Representative Ted Lieu introduced a Space Infrastructure Bill in the U.S. House of Representatives, the lower house of the U.S. Congress. The draft bill directs the Department of Homeland Security (DHS) to designate space systems, services, and technology as critical infrastructure[76]. The draft bill also requires DHS in consultation with relevant agencies (without naming them) to issue guidance on "(1) defining the scope of such sector, with consideration of satellites and space vehicles, space-related terrestrial systems and launch infrastructure, space-related production facilities, and applicable information technology; (2) designating a Sector-Specific Agency for space systems, services, and technology; and (3) identifying appropriate committees and advisories to accompany such sector, including Government Coordinating Councils and Sector Coordinating Councils[76]." It recognizes the lack of coordination and the lack of a single responsible governmental body. However, the bill is still a draft and in the early stages of the legislation process.

The currently designated 16 critical infrastructure sectors are complex and interdependent systems. Such interconnectedness and interdependence may produce unpredicted consequences and major risks. Disruption to a single sector or a supply of a sector may lead to disruption of several other sectors [77].

Satellite Communications (SATCOM)

Communication Satellites have a wide range of applications. They are used throughout all critical infrastructure sectors. SATCOM provides a backbone for the seamless operation of massive machine-type communication otherwise known as the Internet of Things (IoT) devices. The next-generation network of 5G and its infrastructure will heavily rely on

SATCOM. 5G will enable new applications in different industries. Due to the huge increase in IoT devices and their ability to produce and exchange massive amounts of data, satellites help to balance or offload traditional fiber optic networks[78].

International Communication Union (ITU) identified three main development paths for the future of international mobile communication that uses satellite communications: (1) enhanced Mobile Broadband, (2) ultra-reliable and low latency communication, (3) massive machine-type communications. Figure 9 showcases the main applications of each path. The figure was published in the ITU's "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond".

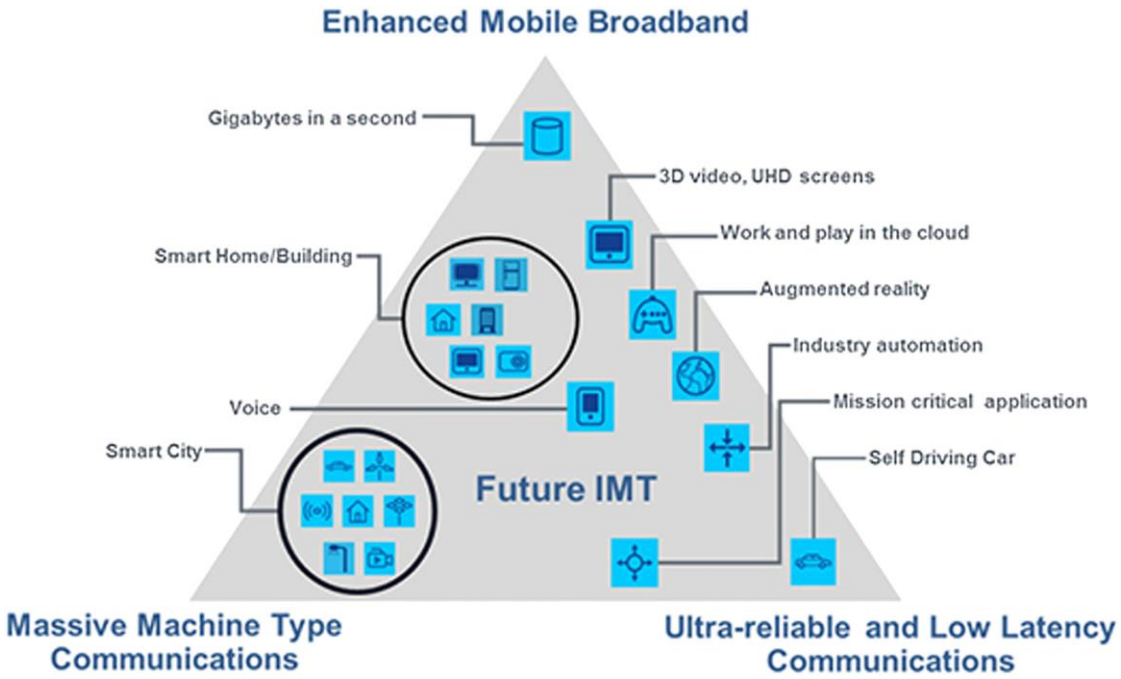

Figure 9: Future of Mobile Communications based on Satellite Infrastructure

Source: Adapted from [79]

Specific applications of SATCOMS use in different industries:

- **Energy Sector** - determining pipeline status through using critical surveillance of oil and gas infrastructure, advanced metering of smart grid sub-system[78].
- **Transportation Sector** - remote Road alerts, assets tracking, transportation fleet management, services to onboard moving platforms such as containers on board a vessel or a train[78].

- **Agriculture sector** - livestock management, farming[78], connecting data producing IoT devices such as weather stations, data from farm machinery, and sensors to business applications[80].
- **Financial sector** – connectivity for remote offices, ATM, remote financial IoT devices, digitalized banking, scalable infrastructure for seamless banking and insurance services[81], [82].
- **Construction and Mining** – satellite-connected IoT devices monitor and manage remote mining and construction sites maximizing safety and finetuning maintenance procedures[81].

Remote Sensing Satellites

Remote sensing satellites can acquire information about Earth, its atmosphere, and other planets and space bodies. There are two types of sensing: optical and radar. The data is being acquired from a distance, using special tools integrated as a part of a satellite and designed to detect and record reflected or emitted energy[83].

There are many applications for remote sensing satellites[84]:

- Observation of the atmosphere for monitoring climate change, pollution, and weather events.
- Monitoring of ocean coastline, sea-level change, marine traffic, mapping of water currents, sea surface temperature, and salinity.
- Exploration of mineral resources, monitoring of weather events such as floods and droughts.
- Deforestation and forest fires.
- Agricultural monitoring of crops and effects of wild animals and weather events on the crops.
- Urban planning: cooling and shading potential, distribution of urban green, mapping, physical aspects of city structure[84], [85].

There is one unique type of remote sensing called **InSAR** (interferometric synthetic aperture radar) that is worthy of special attention. The InSAR technique remotely measures surface deformation with high accuracy at the centimetre to millimetre level[86]. Applications of that type of remote sensing are extremely wide. It can help measure the slightest change in buildings. For example, is the reactor of the nuclear power plant remains in stable condition,

or is it tilting outside of the norm. InSAR can be used in disaster relief and preparedness assessing the threat to infrastructure after a weather event or an act of violence or war.

3.1.6 Satellite Cyber Attacks

Cyberattacks on satellites are not a new occurrence. In 1998 a U.S. communications satellite suffered a computer failure. Affected users were unable to pay for gas, and hospitals were unable to contact physicians who via established communication means such as pagers, and TV stations were unable to deliver programming[31].

However, the vile 2022 invasion of Ukraine by russia gave the cyber threat to satellite communication a much more real implication.

VIASAT operator, which provides internet services to Ukraine and much of Europe officially reported that "On 24 February 2022, a multifaceted and deliberate cyber-attack against Viasat's KA-SAT network resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. While most users were unaffected by the incident, the cyber-attack did impact several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe[87]".

It was confirmed that hackers exploited a misconfigured VPN device to gain access to Viasat's satellite network and cause a massive internet outage on the day of the russian invasion of Ukraine[88].

As VIASAT reported, tens of thousands of modems that were hit in Ukraine abruptly lost Internet connection and did not try to reconnect. "A really huge loss in communications in the very beginning of the war" said a high-ranking Ukrainian cybersecurity official[89]. This is consistent with the threat assessments conducted by the Defence Intelligence agency in 2019 and 2022.

It was also reported that almost a month after the attack, the disruptions of infrastructure continued well beyond Ukraine. In March 2022, thousands were still offline in Europe, around 2,000 wind turbines were still disconnected in Germany, and companies were racing to replace broken modems or fix connections with updates[90].

On March 17, 2022, the Cybersecurity & Infrastructure Security Agency (CISA) issued the alert AA22-076A warning of possible threats to the American and international communication satellites due to geopolitical situation. CISA also provided critical infrastructure operators with mitigation recommendations.[91]

However, it was not the end of the attack. The russian cybercriminals were persistent in their effort to take over communication systems. As late as March 30, 2022, almost six

weeks after the original attack, VIASAT was reporting that the same hackers responsible for the February 24th attack “are still trying to hobble U.S. telecommunications company Viasat as it works to bring its users back online”. The company also confirmed that “a parallel attack was launched at almost exactly the same time [as the first attack]and used "high volumes of focused, malicious traffic" to try and overwhelm Viasat's network and was still ongoing.[92]”

While VIASAT-provided internet was not available, another American company stepped in to provide satellite internet for Ukraine. SpaceX dispatched thousands of Starlink satellites to cover as much of the Ukrainian territory as possible with high-speed internet. This action did not go unnoticed by the russians. Starlink network started to experience jamming of its signal. While jamming is considered more of an electromagnetic warfare technique rather than purely cyber, the threat to satellites spills over into the cyber realm. The Director of electronic warfare for the Office of the Secretary of Defense, Dave Tremper, addressed SpaceX’s ability rapid ability to swiftly terminate a Russian effort to jam its Starlink satellites, which provided internet to Ukraine[93].

3.1.7 Cyber Exercises with Satellite Scenario

Unfortunately, there are not many publicly available cyber exercises that incorporate the space or satellite segment. The assumption is that due to the highly sensitive nature of satellite communication, there are classified cyber exercises that train to defend satellites. While it can be true, it is also important to note that most of the satellite components are made by private companies, this having cyber exercises in the public domain would be beneficial. Curry and Drage [43] suggest that “some outside the intelligence services seem to overestimate the skills and capacity of government and at the same time seem to underestimate the depth and breadth of the vast commercial cyber security industry.[…] private sector can develop their practice at a stunning rate that it is almost impossible to match in the public sector[43].”

The most famous and large-scale cyber exercise in the world - **Locked Shields** includes a satellite component. The cyber exercise is organized by NATO CCDCOE and is held annually in Tallinn Estonia. It incorporates satellite-based scenario as a part of the technical game as well as a part of the strategic decision-making track. The strategic decision-making track allows government executives to think through their actions and response once satellites are attacked and communication lines are severed in the time of the full-scale cyberwar. It is a multinational exercise and is based on fictional geopolitical events and geography.

Jack Voltaic is an American cyber exercise run by the Army Cyber Institute at West Point. The second iteration of the exercise that took place in Houston, TX in 2019 included the telecommunication sector which included satellites. The third iteration of the exercise doesn't seem to include the telecommunication component[94].

Red Flag 21-1 cyber exercise organized by the US Air Force at the Nellis Air Force Base in Nevada integrates space, and cyberspace for joint all-domain operations training. "Space-unit participants include blue, red, and white players from the United States Space Force, U.S. Army Space, and Missile Defense Command, and allied nations' combat air forces.[95]" The exercise is geartowardrds military participants and does not train public-private coordination or iincludecivilian space infrastructure.

In 2021, as a part of the American Institute of Aeronautics and Astronautics space technology conference, **Space-ISAC** conducted a tabletop exercise for the space industry leaders to address a breach of a satellite's ground control uplink. Space-ISAC "said the results of the event […] will shape how the group builds its 24-hour watch center slated to open next year. The wargame also helped to "practice and exercise the muscle movements that are requiretoto execute this [information-sharing] mission"[96].

Hack-a-Sat is a capture-the-flag style of cyber competition. The exercise is managed by the U.S. Space Force and runs for the third year in a row. "Hack-A-Sat is designed to inspire the world's top cybersecurity talent to develop the skills necessary to help reduce vulnerabilities and build more secure space systems.[…] Hack-A-Sat, is open to all cybersecurity researchers who want to up their skills and knowledge of space cybersecurity. This Capture-The-Flag challenge begins with a Qualification Event and culminates in an attack/defend style Final Event.[97]". It is a purely technical exercise and does not include the strategic game.

There are several other hack-a-sat type cyber competitions, but they are very technical, without coordination and decision-making track. While these competitions are still useful, they are beyond the scope of this research.

3.2 Case study design

The chosen methodology for the thesis is the **case study** method. “A case study is an empirical inquiry that investigates a contemporary phenomenon (the “case”) in depth and within its real-world context” according to Yin[98]. The research process followed the proposed sequence of steps as shown in Figure 10.

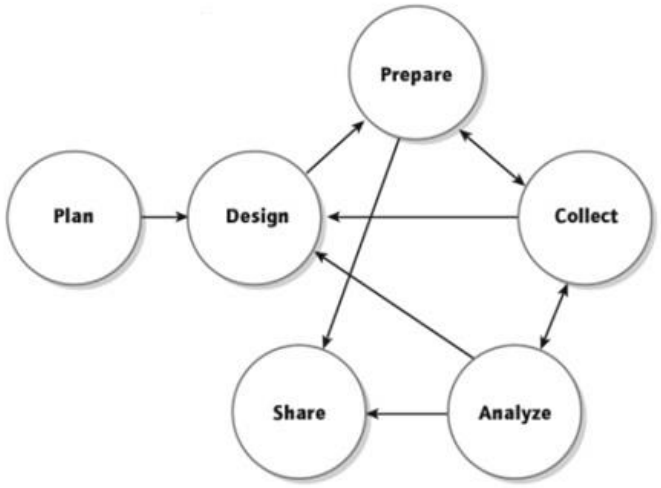

Figure 10: Case Study Research Process

Source: Adapted from [98]

Following Yin’s framework for case study preparation and design, first, the research questions were identified. A thorough literature review was conducted in the initial stage of the thesis to develop an explicit understanding of space industry governance and existing challenges. Several themes were identified, including challenges and opportunities for a public-private partnership, space traffic, megaconstellations, ground station management, space debris mitigation, and the increasing need for international operational standards. The initial literature review clearly established a gap in the nexus of cybersecurity and satellite operations.

As the communication backbone to most critical infrastructure industries, it was surprising how little attention cybersecurity governance of satellites received so far in the United States. Out of observations of trends in cybersecurity breaches (such as increased attacks on critical infrastructure), and literature review it became evident that the satellite industry is transforming into a bigger target for cyber operations. While the industry becomes more accessible, the number of vendors grows, but no new policies are being established for the industry as a whole. The research gap was apparent, and no purely academic literature was

addressing the gap on the policy level. The evidence that cybersecurity governance in the space industry is rather a new and growing body of knowledge with few comprehensive works existing was established. White papers and government reports are not considered a part of purely academic literature in this case.

The initial research question of how the satellite industry is being regulated in regards to cybersecurity seemed to be answered after the first iteration of collecting and analyzing the data. The following iteration of re-designing the study and collecting data combined with the author's professional affiliation in the cyber defense industry allowed for constructing a more insightful research question that the thesis was designed to address. Once the new research question was identified, the appropriate methodology was chosen. The chosen methodology had to allow for the results of this thesis to contribute and move forward in the currently developing scholarly field.

The case study method was chosen as the focus of the study is contemporary real-life phenomena and most of the research questions start with 'what', 'how', and 'why'[98]. The main research question is "How to improve the cybersecurity of commercial satellite industry on policy level" addresses the criteria of the case study.

In addition, the case study should "contribute to our knowledge of individual, group, organizational, social, political, and related phenomena"[98]. Researching and analyzing the urgent issues of cybersecurity governance in the satellite industry contributes to the knowledge of organizational and political phenomena and addresses this criterion.

The nature of the study is exploratory research with the goal to provide insight into the cybersecurity governance of the satellite industry and describe what is the role of cyber exercise in influencing policy and governance processes.

Propositions were developed that support each research question and are logically linked to collected data. Hypothesis was designed based on the propositions.

Research Question 1: How is cyber security addressed on strategic and policy levels in the United States.

Proposition 1: IF there is clarity of existing legal, policy, and operational frameworks THEN it is possible to determine the gaps

Hypothesis 1: Current state of cybersecurity policy and regulation is inadequate. Coordination between government and private sector is ill-defined, not well-practiced and needs to be better streamlined.

Research Question 2: What are the main threats and vulnerabilities of satellite systems?

Proposition 2: IF the cyber threat landscape is holistically assessed THEN it is possible to develop USG integrated public-private cyber policy engagement framework to ensure better information sharing and coordination on satellite cybersecurity with clearly defined roles for federal and commercial entities.

Hypothesis 2: Space threat actors are different from "usual suspects" in the cyber domain.

Research Question 3: How can cyber exercises contribute to cybersecurity policy development for satellite systems?

Proposition 3: IF cyber exercises are useful for policy formulation, THEN the number and complexity of exercises need to be increased and supported at policy level.

Hypothesis 3: Cyber exercises can provide significant insight into the real and urgent gaps in policy decision making.

3.3 Research Methodology

The research employs the case study method. It applies the *triangulation of data* approach to ensure that the thesis attains the research objectives. Combining the use of multiple and complex sources of evidence allows for higher confidence in the results of the research. Logical and compelling results build a strong foundation for relevant conclusions and actionable recommendations that research is set to produce. Four main sources of evidence were used: semi-structured interviews, surveys, literature review, and observations.

First, a vast literature review was performed. To address the objective of identifying existing cybersecurity regulations in the United States (RO2) numerous documents and policy papers were analyzed. The existing national-level space and cyber strategies, policies, and available technical cyber frameworks were systematized. The research identified several policies and legislations that are currently in draft form but are expected to be finalized within a year or so. The systematization of available and anticipated policies and standards allowed for an insightful initial representation of the regulatory landscape of the satellite cybersecurity field. The literature review also analyzed and organized known cyber threats to satellite systems.

Second, semi-structured interviews with prominent cyber experts were conducted. The experts included professionals with experience in cybersecurity, space and satellite systems,

cyber exercises from defense and civilian sectors. A survey among a different set of cybersecurity professionals was conducted as well.

Third, the thematic analysis was performed. All interviews were transcribed to gain a better understanding of the interviewee's perception on the application of cybersecurity standards, but most importantly on possibilities and limitations of using cyber exercises to inform policy change.

3.3.1 Data Collection and Analysis

The main method to establish the credibility of findings through data collection and analysis was a *triangulation of data* by using multiple sources of evidence. The research process included the following data collection methods:

Documentation. As a new phenomenon of merging cybersecurity and space is a subject of the research, there are not a lot of purely academic sources available. To ensure that research adequately addresses this issue latest white papers, draft legislation, and industry reports were used. The research analyzed many executive-level administrative documents and strategies, as well as government reports.

Academic papers and books. There is a well-established body of knowledge on wargaming and cyber exercises, its goals, applications, and shortcomings. Academic articles were reviewed to analyze the development of wargaming as a tool for informing policy and establish its relevance to the cyber realm.

Archival records such as historical records of space activities, national budgets, and other statistical data were used.

Interview results. Seven interviews were conducted with the top experts in cybersecurity, space, and cyber exercise fields. The data was transcribed, and thematic analysis was performed using NVIVO.

Survey results. The survey was conducted and some aggregated insights were used to support data collected through the interviews and desk research.

Participatory observations from regular professional involvement in the field of cybersecurity, cyber defense, and cyber exercises.

3.3.2 Interviews

The interviews were conducted with a diverse group of government, academia, and private sector professionals with experience in the cyber, space, and cyber exercise.. The interviews allowed me to gain a holistic understanding of the field of cybersecurity regulations, space cyber threats, and the attitude towards the use of cyber exercise to inform policy.

Before the interview, each interviewee was informed about the research and its goals. Each interviewee signed the "Interview consent form" where they agreed to be recorded but the recording and the transcript should be deleted after the thesis defence. All interviewees agreed to their names and positions to be used in the thesis. However, several participants then asked not to be quoted directly. For the purpose of complying with their wishes, no direct quotes with attributed names will be provided. Each interviewee is assigned a random letter by the researcher that does not correspond to the order in which the person was interviewed nor the order in which the person is listed in the thesis description.

The interviews were semi-structured which goes in line with the exploratory case study. Each interviewee also received a list of 8-9 preliminary questions before the interview. The interview questions were designed to support the research questions and equip the researcher to better examine the hypothesis. As the interviews were semi-structured, the discussion was not limited which allowed for a more comprehensive and detailed conversation as each interviewee had a very special perspective.

The interviewees were selected based on their professional experience with the issues of cyber exercises, regulations, and space policies. Each interview lasted between 30 minutes and one hour.

The seven interviewees were (alphabetical order, based on the last name):

1. **Commander Jacob Galbreath** (US Navy). Head of the Strategy Branch at the NATO CCDCOE. CDR Galbreath is an information professional in the US Navy, and in his previous assignment dealt with telecommunications including space communications, satellites, networks, and standard IT full-stack. He has participated in multiple cyber pieces of training and exercises.
2. **Mr. Mehis Hakkaja** – is the CEO of Clarified Security – the leading cybersecurity company specializing in red teaming, penetration testing, and cyber exercises.

3. **Mr. Lauri Kimmel** – is the Chief Technology Officer at SpaceIT an Estonian space tech company providing Mission Control as a service for satellite operations worldwide. SpaceIT is a partner of the Locked Shields cyber exercise.
4. **Mr. Silver Lodi** – is the Chief Executive Officer of SpaceIT, an Estonian space tech company providing Mission Control as a service for satellite operations worldwide. SpaceIT is a partner of the Locked Shields cyber exercise.
5. **Professor Rain Ottis** - Tenured Associate Professor, TalTech. Professor Ottis is one of the co-founders of world's largest live-fire cyber exercise Locked Shields. He has seen the exercise from inception until the current scale and is still heavily involved with planning and execution.
6. **Mr. Andri Rebane** – Director of Cybersecurity Department at the newly formed Estonian ICT Centre. Mr. Rebane has multiple years of experience with cyber defense in military and civilian agencies. He has participated in or organized several multinational cyber exercises.
7. **Commander Mike Widmann** (US Navy) - NATO Maritime Command (MARCOM) Defence Cyber Operation Lead. CDR Widmann also participate and organized in multiple cyber exercises including the Locked Shields.

All interviews were recorded, and transcribed and thematic analysis was performed through coding. The interview questions are presented in Appendix 3.

3.3.2 Survey

As a part of the research, a survey was conducted. The survey had 21 questions, both multiple-choice and open-ended. The goal of the survey was to support the research questions. Survey questions closely resembled the interview questions, but some had multiple-choice options for better data aggregation and visualization. The survey was anonymous, no personally identifiable data was collected.

Seventeen valid responses were received during the open survey period. The survey was tailored to a small group of professionals with narrow and deep expertise in cyber exercises, cybersecurity, and space communications.

Survey data provided strong support for the data collected during semi-structured interviews yet revealed some unexpected insight into the perception of cyber exercises. Some

of the survey questions were open-ended, and responses to them were as equally valuable as responses to the interview questions. The survey questions are provided in Appendix 4.

3.4 Validity

The extensive literature review performed by Andreas M. Riege [99] on the validity and reliability of the case study research recommends several measures to increase the soundness of research through applying the design tests of construct validity, internal and external validity, and reliability.

1. To increase construct validity and confirmability of the research data *triangulation approach* was used. Multiple sources of evidence such as interviews, documents, observations, and archive materials were analyzed to protect against research bias. During the data collection phase a chain of evidence was established through the use of interview transcripts, observations, and cross checking of sources of evidence. Raw data, findings, recommendations, and interpretations were preserved for audit and analysis in further research stages.
2. To increase the internal validity and credibility of the research the cross-checking of the results was continuously performed during the data analysis stage. Also, presenting and discussing conclusions and data analysis techniques with colleagues and peers was conducted as a part of the peer debriefing technique to establish credibility.
3. To increase the external validity and transferability of the research, a comparison of the evidence collected with the literature during the data analysis phase was conducted. Specially developed codes were used for analysis. The findings of this research are transferable to other cases as the strong background of regulatory landscape development and threat profiles are established. Cyber exercises are described from a position of policy informing tool that can also be adopted and evaluated against applying it in other industries.
4. To increase the reliability and dependability of the research the peer review of the draft report was conducted. The research process, and procedures along with evidence sources are described and can be repeated by other researchers.

4 Results and Discussion

This chapter presents the results and their analysis. The data collected from semi-structured interviews, survey, and literature was processed and analyzed. Thematic analysis was performed using Nvivo. The chapter discusses results and their interpretation, implications, and limitations. The discussion explores the meaning, significance, and relevance of the results to thesis hypotheses. Some of the results are not directly related to the proposed hypothesis but represent reoccurring themes and will be presented as such.

In the following Chapter 5 – Conclusion and Policy Recommendations, the unexpectedly established themes create constructs for actionable policy recommendations. The in-depth description of the interview process, the justification of chosen professionals, and the structure and response significance of the survey were presented in Chapter 3, subchapter 3.3 Research Methodology.

This research is unique in the sense that it was able to collect observations and experiences of professionals directly involved and experienced in a cross-section of cybersecurity, cyber governance, space, and cyber exercises.

4.1 Results: Interpretation and Implication

Interview questions and survey questions were designed in a way to reinforce each other and support research questions. The discussion of the results interpreted the results and explained their implications. The interpretation of the results answers the question "What do the results say? The implication answers the question "Why do these results matter?"

Results and themes relevant to Hypothesis 1.

1. Attitudes towards Cybersecurity Regulations, Standards, Policies

The research starts with mapping the existing frameworks, strategies, policy guidance, and regulations. When interviewees and survey participants (24 combined) were asked to name what cybersecurity strategies, policies, standards, or regulations they are aware of, more than 40 different standards and regulations were mentioned. The most often cited was the combination of IT-Grundschutz, ISKE, and E-ITS as many participants were from Europe. The second most cited standards were the family of ISO27K standards on how to manage information security. The third most cited was NIST produced cybersecurity standards and Cybersecurity Framework. MITRE ATT&CK also got mentioned quite a

number of times. Strategy-level documents such as NATO cyber doctrine or SPD-5 were mentioned only twice.

Interviewee E expressed concern about the number of regulations and their actual use. “[ ] from one side, we have many regulations, they are very long, they are very descriptive, but they don't actually give too much to the actual cybersecurity, where you have different methods how to protect yourself. [ ] there's so much more behind those, even if you take the ISO 27001 - it's very high level, but you need to go very deep into the Active Directory policies to actually implement the real cybersecurity and, and I think we don't have very good baseline methods for that”.

On the other hand, Interviewee D noted a difference between layers of cyber regulations and suggested that “[ ] cybersecurity regulations are too technical. […] Focus at the middle management level. […] there's a lot of strategic policy guidance. There's a lot of technical guidance, but how to make the two work together is missing. That's why there's the tendency to either provide too many policies that don't really become effective or sometimes even contradict each other. And then you have a lot of technical policies and technical solutions, and then it becomes chaotic, because it depends on who issued what and when, what the objective was. [ ] There is not enough and there's too many [regulation] depending on the scope [ ].”

Figure 11 showcases that survey participants were united in the believe that more cybersecurity (CS) regulations do not make industries less secure. Almost an equal number of respondents agreed with a definitive statement that more CS regulations lead to more security. While it is difficult to get the ratio right, generally more regulation is better than less.

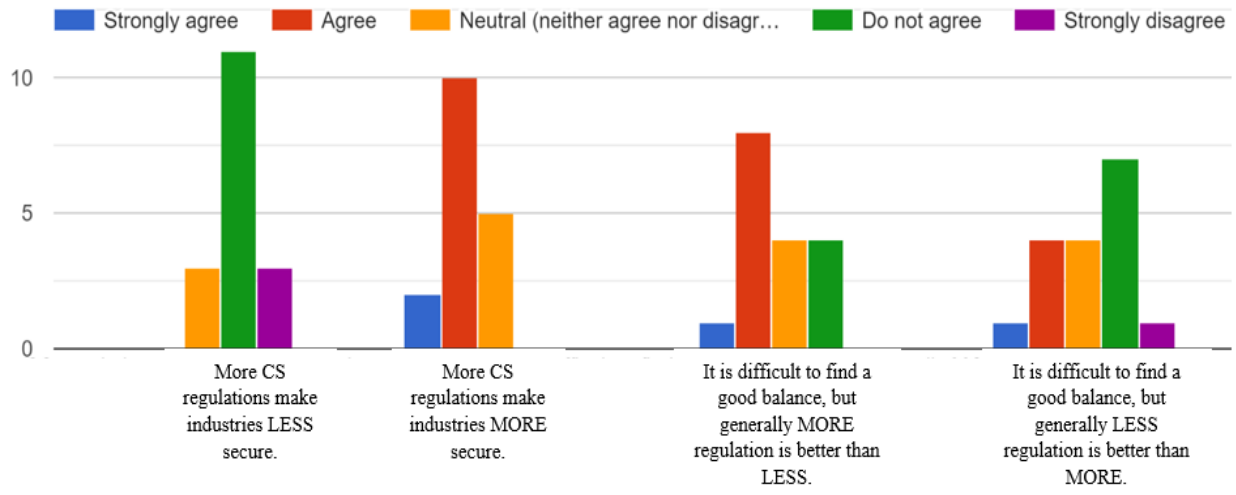

Figure 11: Survey question assessing general attitude to the number of cybersecurity regulations

Source: Author

While every participant named some standards and regulations, 10 people said they are not applying any cybersecurity standards or policy guidance in their everyday work. One survey respondent even wrote "Nope, only common sense and knowledge".

Discussion: The responses indicated the significance and applicability of internationally recognized technical cyber standards (some of which are voluntary). It also illustrated that the knowledge and availability of standards don't automatically translate into their regular use. Even though there are many existing technical regulations there are still gaps that need to be standardized and regulated better. Cybersecurity professionals that work in this field every day perceive the level of regulations and policies development differently. There is general trend to need and require more cybersecurity regulation.

The results are important because they highlight the need for an enforcement mechanism for the standards, not just their availability. In Europe, arguably, the General Data Protection Regulation (GDPR) is the enforcement mechanism. Even though GDPR is not a cybersecurity regulation per se, an organization needs good cybersecurity practices to comply with the GDPR. In the United States, a similar mechanism to GDPR does not exist.

The results also indicate that professionals dealing with technical standards think that more managerial level regulations are needed. Cyber professionals in managerial capacities think that there are too many high level policies and that more technical and specific standards need to be developed. The cybersecurity field is still in its early development stages

if even the people who are supposed to speak the same language see different gaps. More standardization needs to happen, as well as a better assessment of new regulations. The new regulations, standards, and policy need to be carefully evaluated in order to not overlap or contradict already existing guidance. Industry regulating bodies and responsible government agencies should not be afraid to overproduce cybersecurity regulations at this stage of industry development. It is clear from the literature review, interviews, and the survey that there is demand for more precise guidance.

2. Level of cybersecurity regulations

All participants of the survey and interviews agreed that the level of cybersecurity regulations depends on the industry and is not universal across the board. Interviewee A suggested that government-level regulations should come only if the industry doesn't produce anything on its own. Otherwise, regulations and standards should come from within the industry.

When asked to rate major industries on the state of cybersecurity regulations, the survey participants generally agreed that the communications sector, banking and financial services sector, and the defense sectors are sufficiently regulated. They were also offered the option to indicate which industry is overregulated. Two industries stood out: the space industry and IT and software development industry. Zero respondents indicated those industries to be overregulated. Survey results are presented in Figure 12. The results are consistent with the literature review analysis on the lack of cybersecurity standards in the space industry.

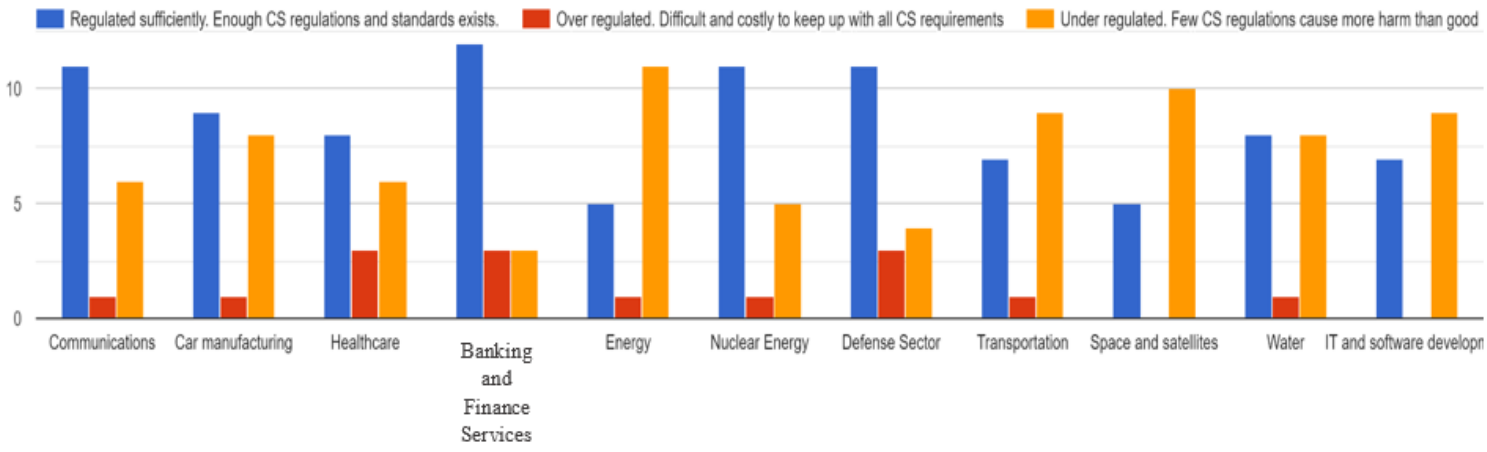

Figure 12: Survey responses indicating the state of cybersecurity regulations in each industry.

Source: Author

Discussion: The results indicated that some industries are doing significantly better than others in terms of cybersecurity development. It was expected to see that the space industry is in need of better regulation. However, the results showed unexpectedly that the software development sector is under regulated as well, according to many participants.

The results imply that that there is still a lot of work to do in terms of standardization and securing critical infrastructure. The perception of what is enough or not enough regulation also differs as some industries got an equal or almost equal assessment score for "over regulated" and "under regulated".

3. "Layers" of cybersecurity regulations and compliance.

Cyber compliance is costly. An organization needs to hire more people and acquire more resources in order to be cyber compliant. This is universal and translates well in any country. Several interviewees suggested that cyber regulations are easier and more doable for large companies to comply but are too restrictive for small companies.

Interviewee B elaborated on the challenges to small and medium-sized enterprises (SME). "[Cybersecurity] regulation is quite well established for the big players. [ ] if you're a large bank, if you're a large multinational corporation, there's regulation that applies to you internationally as well as in all the nations that you operate in [..]. However, where we do have a problem is on the lower end of the spectrum, so we're talking about the smaller companies, smaller entities [..]. [SMEs] face many of the same problems and in some cases, they faces many of the same regulations than the vast multibillion, multi trillion companies do. [ ] we don't have, good regulation for this lower end of the spectrum. Something that would be doable with finite few resources to get the most bang for the buck, and then just accept that they will not go as far or as deep as the companies that can throw millions or hundreds of millions on the cybersecurity budget. [Small companies] for sure are having trouble, even if they do realize that there was regulation and recognize the need for it. They probably don't have the resources. There's just not enough manpower out there to solve all these things."

Interviewee A suggested that cybersecurity compliance of SMEs should perhaps be gradual, with different maturity level requirements and different rigors of assessment. The level of cybersecurity compliance should be based on the size, impact, and mission of the company. Not all companies should be "military grade" in terms of cybersecurity. Tailored compliance eases the pressure and adjusts cybersecurity requirements to the task, rather than to an elusive state of ideal compliance.

On flip side, there are regulations for the sake of having regulations, or to appease the public and executive governing body. Several interviewees shared this sentiment. For example, a regulation to report cyber security breaches to the government. In one European country the threshold for reporting is so high that only a small number of companies have ever had to do it. The regulation is in place, but its value is almost non-existent.

Discussion. The results show that the substance of the regulation is important as it highlights the importance of substance over availability. The results are important as they indicate there is no "one size fits all solution", and that governing bodies need to consider those intricacies in order to enhance the cyber security of an industry rather than hamper the growth of SMEs with unreasonable cyber compliance demands.

4. Public-private partnerships

Only one interviewee discussed cyber regulations from a public-private partnership perspective.

"ISACs and CISA in the US are trying to get the government and private industry together, to share information. It's not regulated, it's promoted, it is good practice." It was also noted that the success of such information and threat intelligence exchange platforms are highly dependent on the personalities of people managing the program.

Discussion: The results indicate that government agencies are not viewed as partners by the majority of people. Only one person talked about partnership. This indicates that government agencies need to build better relationships with the private sector that is not solely based on contractual collaboration. Sharing cyber threat information is CISA's responsibility but similar models can be replicated with other leading agencies.

Hypothesis 1: The current state of cybersecurity policy and regulation is inadequate. Coordination between governments and the private sector is ill-defined and needs to be better streamlined.

Based on the results, this hypothesis is a two part issue. The results of the literature review, interviews, and the survey indicated that, indeed, the current state of cybersecurity policy and regulation is inadequate. More guidance and regulations – and for different levels including managerial – are needed. The first part of the hypothesis accumulated enough evidence to prove it.

The second part of the hypothesis, about the government and private sector coordination, produced somewhat mixed results. There are many attempts to cooperate.

For example, NIST closely cooperates with the private sector on producing specific risk-based highly technical cybersecurity guidelines. CISA cooperates with the private sector more on the managerial level, but it still provides technical advice. The Space ISAC is a new organization, founded only in 2019 and opened to general membership 2020 with very small staff and resources. However, they have an opportunity to build a strong foundation for threat intelligence sharing and experience exchange. The evidence is mixed. While it appears that currently coordination between public and private sectors in the US may be ill-defined, there are appears to be efforts to strengthen that cooperation. The second part of this hypothesis is only partially correct.

Results and themes relevant to Hypothesis 2.

5. Cyber threats in Space

When asked about cyber threat perception in space, most of the interviewees agreed that space is expensive. Even though there is increasing use of COTS devices and software, most of the military technologies are still proprietary and require deep technical knowledge to gain access to or compromise (Interviewees A-G). Interviewee D pointed out that a vulnerability in VIASAT system, for example, will not be relevant for SpaceX system.

Interviewee C said that "Space systems are still software systems. There may be a bigger reward regarding news value if you take down a satellite system, but in reality, the people who could attack your satellite system are still the same who are attacking the banking

industry or IT networks. Maybe there is a little barrier because of [satellite] domain knowledge. People must know more about satellite communications and how things work."

Interviewee B also noted that while satellite systems are complex and require specialized knowledge, the "office side" of the satellite business remains the same and is vulnerable to similar malicious activity as the office side of any other business.

Survey responders also agree that Russia and China, as state actors are the strongest threats to satellite systems, while script kiddies and hacktivist poses the least threats. Survey findings are presented in Figure 13.

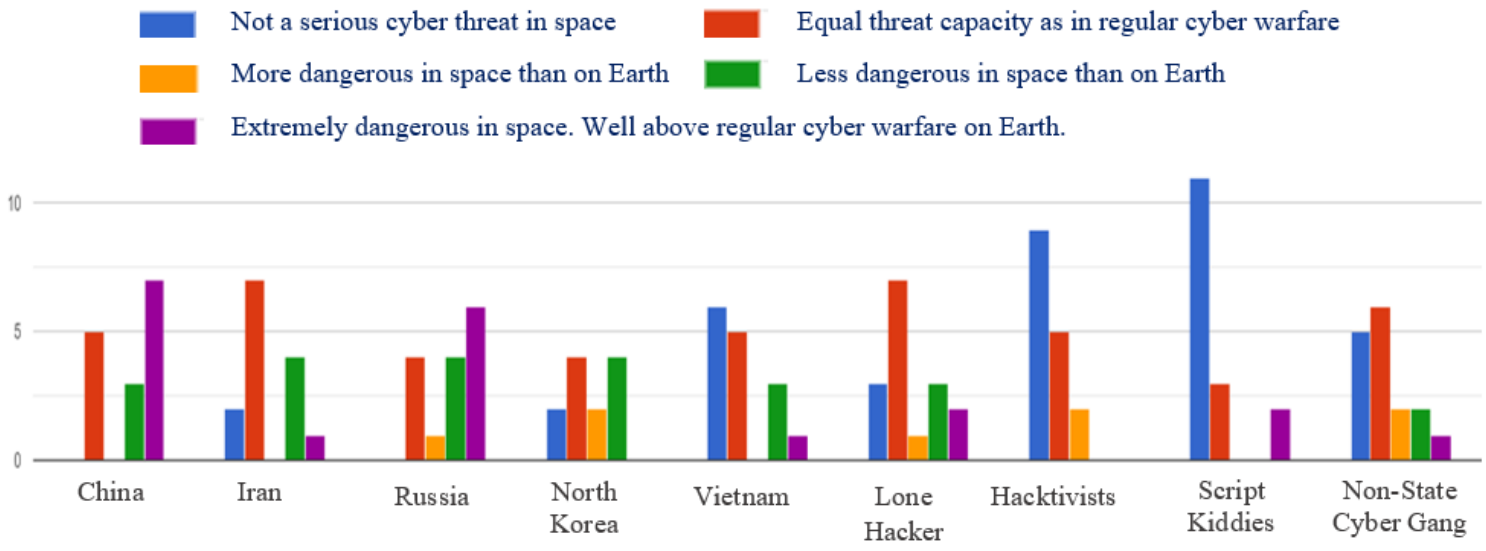

Figure 13: Most dangerous cyber threat actors to satellite systems

Sources: Author

While the United States can also be considered a major cyber threat for space satellites due to its extensive use and familiarity with existing technology, it is not mentioned in this thesis as an option. Parts of this research are U.S.-centric and the United States is treated as peaceful rational actor.

Discussion: The results indicate that there is no confusion who the enemy is and what capabilities the enemy needs to possess. Since interviewees and survey respondents were from North America and Europe (all NATO members), the results show that the threat perception is shared, and no extra persuasive measures need to be taken to convince other partner nations. While it requires extra knowledge and efforts to hack a satellite system, one does not need special preparation to hamper the business activities of the satellite operator. The results are significant especially in terms of recent geopolitical events and different threat

assessments of the adversary by NATO member states. While nation state threats are clear, it is important to keep the "back end" of business running as securely as the highly secure satellite systems. Cyber hygiene and vulnerabilities patching should be carefully applied to the business side of operations as well.

6. Commercialization of space diversifies threat actor profiles

Space was not a lucrative industry for financially motivated cyber threat actors, but it is changing. While all interviewees generally agreed that at the current development stage space and satellites are targets for nation states, one response proposed to look further in the future and be prepared for it.

Interviewee A stressed that the commercialization of space will bring more non-state attackers into that industry. In in the past maybe lone hackers were working for the state and were getting paid by the state, then now situation changes. When there is money and financial gain, there are always more actors who want to illegally gain those financial resources.

"The key thing for cyber criminals is how to monetize? [..] Who's the buyer? It's easiest if it's a state actor interested in getting some foothold. If it's North Korea that may have its agenda or if they're willing to pay for having a foothold, or opportunities in space, through hacking, then this is monetization."

"The big money comes when there's a big ecosystem". There are so many companies in a bad state of cybersecurity, and they don't even realize it. Hackers pay attention to that. "There are so many opportunities to monetize" on Earth, that space is not yet needed.

Now there are few companies, and the rest are government agencies that manufacture or operate satellites. For a financially motivated attacker, it is not interesting, as it is very difficult to monetize. However, once there are hundreds of commercial companies with thousands of satellites that are wealthy enough to extort money from, then it gives "more opportunities for bad guys to make money off of this segment."

Discussion: The results indicate that the state of cybersecurity is constantly changing. Governments and private companies need to be aware, think forward and prepare themselves for more cyber-attacks as the industry diversifies. The results are important as they provide an interesting insight into how the cyber future of the satellite industry will look like. Will ransomware become a usual occurrence in space? Or will the necessary guardrails be implemented to ensure space stays secure for decades to come.

Hypothesis 2: Space threat actors are different from the "usual suspects" in cyber domain.

The hypothesis is disproved. Space threat actors are the same as large well-known regular cyber adversaries. Thought not all strong terrestrial cyber actors are as impactful in space, thought.

Results and themes relevant to Hypothesis 3.

7. Cyber exercise as policy informing tools

Similar to the question about cyber threat actors in space, when asked about using cyber exercises for cyber policy planning, all interviewees and all survey respondents recognized the importance, the role and the impact of cyber exercises. It is consistent with the literature review that in detail discusses different types of cyber exercise and their application on different stages of policy planning. What most interviewees and survey participants emphasized is not cyber exercise ability to provide policy insights but the quality of implementation of those insights. Interviewee E provided a detailed explanation of the phenomena. The tricky part is "how we actually implement those into lessons learned into new policies, new legislation. [..] What we see from data science is that you might have 10 years of the same lessons identified, and no one really wants to change anything. Maybe after 10 years, […] the legislation to improve our security posture [will be introduced]. It will take place eventually."

The interviewee also shared the sentiment of survey responders that the technical side of exercises is much easier to implement then any strategic and policy findings. "[It is] three to five years for most nations to actually change something [policy wise] and learn from the exercise."

Discussion: While cyber exercises are recognized as a good tool for policy making, it appears that the processes are not well prepared to accommodate change quickly. It is much easier to implement change on an organizational level when managerial buy-in is present, rather than on the government level when many people need to agree, and some are lacking understanding either of cyber security or cyber exercises. Technical changes are easier to implement than policy changes. The results indicate that there is a lot of work to be done to smoothly integrate cyber exercises lessons-learned in the formal policy planning process.

8. Private sector participation in joint cyber exercises

Based on observations and interviews it became apparent that some private sector companies manufacturing hardware or developing software that can be dual use are somewhat hesitant to participate in cyber exercises. It is due to the unfounded believe that being breached will negatively impact the public perception of their product. On the other hand, there are companies that recognize the value that "free pen testing" adds to their products. Those companies use it to market their products as very secured as they had a chance to test and address major vulnerabilities.

As interviewee D suggests "[private companies] are a little bit more hesitant to use [their products] for exercises, because if vulnerabilities are found this could hurt their image. Many companies are like this, whether it's good or bad, depends on the company. Some companies […] like to be able to use their gear. Because if they find vulnerabilities, it's free for them, then they can fix it. And then they will turn this around as a sales pitch to other entities and saying: "All these government officials have used our stuff and it worked."

Discussion: The results indicate that even companies in the IT industry are not well versed on the advantages of participating in cyber exercises. This point echoes the previous results on public-private partnership. There is more to be done to coordinate and integrate government and private cyber defense training efforts.

9. Understanding of the goals of cyber exercises.

This turned out to be quite an interesting insight. All interviewees, from both space and cyber industries have participated in cyber exercises several times. However, not all survey respondents have participated in a cyber exercise. Note, all survey respondents were either from cyber or space industry or both.

Out of 14 cybersecurity professionals only 4 never participated in cyber exercises, but were aware of them. The responses to the understanding of the goals of cyber exercises were specific. For instance, one respondent wrote that the goal of a cyber exercise is to "Ensure all levels of command understand their roles and responsibilities during a major cyber incident. This includes whom to coordinate with outside your organization, having mechanisms and procedures to pass relevant information internally and to external partners. And being able to explain the consequences of the cyber-attack to senior level personnel in a manner that is meaningful. Also being able to convey that same message to a public audience without

causing unnecessary panic as they may not have any cyber understanding." This is consistent with several Interviewees (B, D, E, G) that also emphasized coordination and communication as main benefits of cyber exercise. "Collaboration between different stakeholders is invaluable. Understanding each other's approach to a cyber incident expedites the solution" added another survey responder.

Eight responders indicated that they work in the space industry. Out of those eight people only four participated in a cyber exercise before. Those four also the same respondents that work in the intersection of space and cyber. They indicated both industries as their professional engagement. The space industry professionals that never participated in cyber exercises expressed low level of awareness of the goals of cyber exercises. Most only noted technical side of cyber exercises as the main goal. One responded that that "[my] Organization does not see a need to take part in cyber exercises."

Discussion: While cyber security professional express high level of awareness of cyber exercises, space professionals do not share the same experience. The results indicate that the space industry is not as well integrated in large scale cyber training processes. It is important to realize that the gap between space and cyber exists, and more space professionals and companies need to be included in cyber exercises.

10. Availability of cyber exercise with space segment injects

When asked to name unclassified cyber exercises with an integrated space or satellite scenario, the Locked Shields and Hack-s-SAT type exercises came up the most in the survey. All Interviewees (A-G) noted that due to the sensitivity of the subject, the majority of cyber exercises with a space element are most likely to be classified and highly tailored to an agency that conducts such exercises. It is consistent with the literature review, where few cyber exercises with satellite component were found. However, one Interviewee noted that some disaster relief exercises are considering adding cyber and space layer to their scenario. It is also consistent with what CISA is implementing with their national level rapid reaction exercises.

Discussion: The results indicate one of two things: either there just not enough cyber exercises that integrate space systems or that there are plenty of those cyber exercises, but they are all classified. The most likely explanation is that there are few cyber exercises with a mix of terrestrial and spatial systems and coordination components. It implies that there is a

training vacuum for such exercises with strategic scenarios and technical infrastructure to resemble real life satellite disruption attacks.

11. Practical take aways from cyber exercises.

When asked about the *most valuable insight* from participation in cyber exercise, the survey responses were compelling. The respondents said (direct quotes):

- The value of chaos. Logs must be monitored
- New angels, new ways to look at things or situations
- Proper monitoring and tools to enforce your decisions must be set up first.
- Preparation and training is key. "You go to war with the army you have."
- The response must be well coordinated between responding entities.
- Effective communication, team structure and collaboration is key. There can be many technical experts on the team, but if they are not effectively communicating and there is a lack of good leadership, technical expertise won't help.
- Aware of the vulnerabilities in the system and potential consequences
- Just 'an IT guy' does not have enough competences to understand the content of a satellite system. He needs special training.
- Thresholds, type of threats, actors, means and methods.

The interviewees echoed similar sentiments with a stronger emphasis on communication and networking that participation in cyber exercise provides. Several interviewees (A, D, E, G) noted that participation in cyber exercises allowed them to make professional contact they would other wise not be able to make. This type of intergovernmental and public-private networking is invaluable in a time of crisis response.

Discussion: The insights respondents were able to take away are either technical, tactical, or strategic. That indicates that cyber exercises are evolving from simple “technical” to a more complex, multi layered events. This wide range of experiences is important to showcase the value of such events to policy makers as well as private entities.

12. Cyber exercises lessons learned

When addressing an organization's ability or experiences with adopting lessons learned, the results were mixed. One survey respondent wrote in that in their experience: "For some exercises the final report can already be written before STARTEX: we learned a lot, we cooperated extensively, etc. Self-criticism is not very popular though it should be seen as a virtue, or not, as long as the end result is that the deficiencies in systems are spotted and fixed/mitigated". While this is quite possible, no other survey responder or interviewee related similar issues. The literature review also did not corroborate that note. Perhaps this was an isolated incident that the participant experienced. The evidence does not support this practice as widespread.

41% of survey respondents noted that in their experience their organization usually conducted an after action review but implemented only some of the recommendations.

Interviewee B also noted that each organization is different in terms of its ability to learn based on cyber exercise participation. "[Some organizations] really don't learn anything from an exercise. They just treat it as an obstacle that was put on their way. [..] There's no learning built in. Learning is incidental. That might happen at an individual level, but not on an organizational level[...] On the other hand, there are organizations that very methodically are trying to figure out how the learning process should help them. They build in reporting, they have their own internal correction review, they write the report, they adjust based on what happened in the exercise. [The range] is really wall to wall."

The need for better lessons learned process is also true for organizers of cyber exercises, especially multinational cyber exercises. It is important to plan the lessons learned processes carefully, from the very beginning of the exercise. It is vital for regularly occurring (annual or bi-annual) exercises to have a lessons learned action plan to be incorporated into next year's initial planning. Producing an analysis of an exercise without using it to build or influence a subsequent exercise is a poor practice equivalent to a business not listening to the concerns of its customers.

Discussion: The evidence of mixed results showcases that the organizers of cyber exercises need to pay more attention to involving participants into the lessons learned part of the exercise to ensure the maximum value from the event. It is true for joint and company-specific cyber exercises. The significance of this finding underlines the importance how cyber exercises are presented to target audience. It should not be discussed as a one or two day event.

The cyber exercise should be presented as a cycle, where preparation, participation and analysis are all important part of successful completion.

13. Limitations of cyber exercises

Several participants expressed their apprehension that there is the perception that the only impacts of cyber exercises was positive. There were drawbacks. One survey respondent wrote in that "Most decision [makers] (especially on [government] level) are very distant from understanding the real threats in the space market. The cyber security is very technical and too complex for most people". The theme of cyber security being a complex and technical subject that senior executives are not comfortable to tackle was voiced in several interviews as well.

Another limitation mentioned was the short preparation cycle and lack of coordination within the participating organization. When considering a large government institution, sometimes the invitation for cyber exercises comes to the wrong department and the team with the wrong type of skills is put together for the exercise. Even when organization recognizes the importance and value of cyber exercises, it is still possible to fail due to competing priorities and no dedicated staff to coordinate cyber exercises (Interviewee E).

Discussion: The results show that limitations to the impact and implementation of cyber exercise certainly exist. However, none of the mentioned limitations are detrimental. These limitations are more pain points that can be addressed. It is important to see that participants of cyber exercises are able to clearly see the existing gap.

14. Real life policy changes due to cyber exercises

The research aimed to identify a direct connection between a cyber exercise and a policy change. One interviewee said that "[honestly] I don't think the exercises raise to the point where they're changing policy." Several Interviewees suggested that policy change doesn't come from one single exercise, and often cyber exercises bring the change gradually. If we omit the technical part of the exercise, the effect of a cyber exercise on policy decision makers is not tangible and difficult to quantify.

One of the examples was how Locked Shields was a contributing factor to the Solarium Commission report. Several members of the Commission visited the exercise and were briefed on its scale, impact, and significance. Once the Solarium report was out, it had two specific

recommendations pertaining to cyber exercises "*Enabling Recommendation 3.3.4: Expand Coordinated Cyber Exercises, Gaming, and Simulation. Enabling Recommendation 3.3.5: Establish a Biennial National Cyber Tabletop Exercise*"[100]. While it is difficult to establish or prove a direct causal link, it is evident that practical exposure to cyber exercises makes an impact on policy makers. Naturally, the Commission members probably visited other cyber exercises as well.

The literature review suggested that there are some tangible results that can be produced through a wargaming approach to solve specific business related tasks. Companies and corporations that procure exercises to solve a specific business need are usually the once that implement the outcomes the best. Interviewee B confirmed this observation in connection to cyber exercises as well. "[…] the most impactful [cyber] exercises that I've seen, from an organizational perspective, have been the ones that are tailored to the specific organization." This is a good indication where cyber exercises can be headed.

Discussion: The results indicate that cyber exercises can impact policies and standard operating procedures on the level of an organization. The results also indicate that cyber exercises have the potential to shape opinions of policy makers on the national level. There is still a lot of work to be done for cyber exercises to mature enough to be considered as a strong policy making tool by decision makers. From the point of view of decision makers, there is also work to be done to develop expertise and awareness to shape cyber exercises in a way that can help answer the most pressing policy questions.

Hypothesis 3: Cyber exercises can provide significant insight into the real and urgent gaps of policy decision making.

The evidence suggest that this hypothesis was confirmed based on the literature review, interviews and survey responses. The evidence are strong and encourage further exploration of cyber exercises applications.

4.2 Limitations

The two major limitations of the research were access and scale. The research was conducted without the ability to access the internal knowledge of CISA and the U.S. Space Force. While the literature review and desk research revealed a lot of information about the

activities of the two agencies directly related to the topic of research, the research would greatly benefit from having access to officials from those two U.S. Government agencies.

Another limitation is the number of survey respondents. While there was never an anticipation to get hundreds of responses due to the novelty and sensitivity of the field, the 17 valid responses only scratch the surface of the vast knowledge and experience base that exists but is still untapped. If similar surveys were conducted on behalf of NIST or another major US agency, the results would have a much stronger evidence base.

The bias of the researcher did not play a role. The researcher had no preconceived opinion on the state of cybersecurity in the satellite industry. Through several rounds of feedback and iteration the research questions and study design came to exist. The researcher's bias could perhaps be dissected in the policy recommendation section. Throughout the rest of the thesis, the facts and opinions of other are presented separately.

The limitations of the results of the research includes the inability of data to expose failures resulting from employing cyber exercises. All literature reviews, survey respondents, and interviewees were only aware of the positive sides of cyber exercise training and its policy implications. There were no studies or documents found that would discuss the negative or unsuccessful cases of cyber exercise results. The literature discussing the negative impact when the results of the games were not implemented was identified. However, that is not the same as having evidence of cyber exercise as a policy informing tool being unsuccessful.

5 Policy Recommendations and Conclusion

This chapter will provide practical, succinct, and actionable recommendations based on all the evidence gathered. Recommendations are U.S. specific.

5.1. Policy Recommendations

On The National Level

Recommendation 1: Designate theSpace sector as the 17th Critical Infrastructure Sector.

Recommendation 2: Task CISA with mapping standards, guidance, and policies for cybersecurity of the satellite industry. Coordinate with DoD to standardize cybersecurity requirements for government satellite service providers.

Recommendation 3: Clarify and streamline existing cyber standards, identify gaps, overlaps, and remove occasional discrepancies. Distinguish cyber standards for SCADA systems and office systems.

Recommendation 4: Improve the cybersecurity of satellite industry supply chains by designing specific technical regulations to address design and development stages of commercial of the shelf (COTS) hardware and software manufacturing.

Recommendation 5: Established a multilayered approach to mapping and assessing cyber regulations. Include technical, tactical, and strategic level guidelines. Technical cyber professionals, mid-level managers, and senior executives should have clear guidance or other types of regulation allowing them to adequately understand and address cybersecurity issues.

Recommendation 6: Establish enforcement mechanisms for existing voluntary cybersecurity regulations in close cooperation with commercial partners, including SMEs and space start-ups.

Recommendation 7: Strengthen public-private cyber threat sharing platforms. Include more SMEs.

Recommendation 8: Establish regular communication platform and designate working level points of contact for public-private coordination activities.

Recommendation 9: Update the 2019 National Emergency Communications Plan with better defined roles and responsibilities for users of satellite communications on the national, federal and local levels.

Recommendation 10: Incorporate the space segment into the list of CISA cybersecurity situational manuals, cyber physical convergence scenarios, and tabletop exercises.

Recommendation 11: Integrate satellite attack scenarios into the Cyber Storm national cyber exercise. Make this exercise an annual event.

Recommendation 12: Introduce space and satellite cyber-attack scenarios to every national and state level crisis preparedness exercise.

Recommendation 13: Establish a POC for cyber exercises coordination withing each federal and state agency.

Recommendation 14: Strengthen Space-ISAC's (cyber threat Information Sharing and Analysis Center) role and establish afield office in Washington D.C for better coordination of policy issues.

Recommendation 15: Improve tools and processes to assess and incorporate lessons learned from exercises into the interagency policy planning activities

On organizational/agency level:

Recommendation 16: Establish a cyber exercise coordinator role within an organization.

Recommendation 17: Define expectations for cyber exercise participation as learning outcomes, not as a win. Establish clear understanding that failure in a national or multinational cyber exercise is an option sometimes better than winning the exercise.

Recommendation 18: Refrain from participating in as many cyber exercises as possible. Have quality preparation/execution/lessons learn cycle within organization implemented well, rather than constantly participating in different exercises and hope for accidental learning.

5.2. Prospects for Future Work

Due to the limitations of scale and access this research only scratched the surface of the endlessly complex, interconnected, and multi-layered satellite industry.

The field of cybersecurity governance in the space industry is new, therefore there are plenty of direction for research. For instance, a deeper look into public-private partnership cooperation is needed. As it is, U.S. government policy to increase procurement of space

services from private companies, the landscape and nature of relationship will also evolve and change. Identifying potential shortcomings and creating a framework for this kind of multi-billion dollar cooperation is a useful scientific effort. Defining how cybersecurity regulations fit into this framework and what role they should play in granting government contracts is also an impactful field.

Interagency cooperation of civilian and military agencies that often use the same commercial satellite provider for similar services should be studied in more detail. Is there an overlap or disproportionate different cybersecurity requirements?

Each satellite segment requires its own research project, as cybersecurity threats for ground stations are different from the space segment. Also, researching more into the space-as-a-service cloud based commercial offers and technical architecture may pose additional security vulnerabilities not present in traditional cloud infrastructure.

There is a vast research field on the spillover effect of satellite cyber-attacks. What would the U.S. tolerate if a cyber-attack on foreign infrastructure interferes with U.S. communication abilities? What would U.S. tolerate as a collateral damage should a need for a cyber offensive operation arise?

Following up and assessing implementation of the Solarium Report and the cybersecurity budgets allocated for cyber defense is another avenue for research.

The most promising research direction is to describe more tools and options on how to improve cyber governance of the satellite sector. Cyber exercises are a good solution, but not the only one. Other policy tools need to be assessed in relation to their use in strengthening cybersecurity governance in the satellite industry.

5.2. Conclusion

The research conducted for the purpose of this thesis was a holistic effort to look at the current state of cybersecurity governance in the satellite industry. Cyber exercises were selected as a tool to assess and inform policy planning. While this research was of a global nature, the focus of its recommendations was tailored to the United States. This section concludes the research and summarizes a direct response to every research question that was guiding this paper.

Every research objective of the thesis was accomplished.

Research objective 1 was to develop integrated policy recommendations for strengthening cybersecurity in the U.S. satellite industry. Policy recommendations are provided in subchapter 5.1.

Research Objective 2 was to identify existing cybersecurity regulations for satellites. Sub chapters 2.1, 3.1,3.2 and 3.3 fully address this objective and describe near future expectations for the legislative process on the issue of satellite cybersecurity.

Research Objective 3 was to develop a comprehensive description of major cyber threats to satellite systems. That was competed in Chapters 2 and 3.

Research Objective 4 was to determine the impact of cyber exercises "lessons learned" on informing policy decision making. Chapter 3 and 4 achieved this objective.

The main research question was how to improve cybersecurity governance of satellite industry. The research found that cyber exercises along with strengthening public-private cooperation are good tools for creating and strengthening existing governance frameworks. However, it is important to consider the human factor and ensure that appropriate points of contacts are established within companies and government agencies, with clear rules and responsibilities.

Research Question 1: How is cyber security addressed on strategic and policy levels in the United States? The short answer is that it is addressed in an inconsistent manner, and that some industries enjoy more and better regulations the others. There is plenty of consolidation and coordination work that needs to be done to harmonize existing strategies and regulations.

Research Question 2: What are the main threats and vulnerabilities of satellite systems?

The main threats are nation states, namely russia and China. However, North Korea and Iran should be followed very closely. While at this stage the space sector is mainly concerned with nation state malign activities, it can soon change. Commercialization of the industry leads to more financially motivated attackers being interested in monetizing on its vulnerabilities.

Research Question 3: How can cyber exercises contribute to cybersecurity policy development for satellite systems?

Cyber exercises can contribute through identifying appropriate scenarios to play, incorporating the space and satellite segment in every disaster or crisis preparedness national and state level exercise. Ensuring every large scale cyber exercise within agency or interagency has a space injects, space cyber physical systems and satellite strategic injects. It is also important to ensure that lessons learned from exercises are formally incorporated and discussed as integral part of policy planning activities.

References

[1] "US Announcement--July 1955." https://history.nasa.gov/sputnik/14.html (accessed Apr. 29, 2022).

[2] "Explorer 1 | Home Page." https://explorer1.jpl.nasa.gov/ (accessed Apr. 29, 2022).

[3] United Nations Office for Outer Space Affairs, "Online Index of Objects Launched into Outer Space." https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id= (accessed Apr. 29, 2022).

[4] "Frequently Asked Questions (FAQs) | Federal Aviation Administration." https://www.faa.gov/space/additional_information/faq#commercial2 (accessed May 04, 2022).

[5] "Commercial Space Data." https://www.faa.gov/data_research/commercial_space_data/ (accessed May 04, 2022).

[6] W. Peeters, "Evolution of the Space Economy: Government Space to Commercial Space and New Space," *https://doi.org/10.1080/14777622.2021.1984001*, vol. 19, no. 3, pp. 206–222, 2022, doi: 10.1080/14777622.2021.1984001.

[7] M. N. Sweeting, "Modern Small Satellites-Changing the Economics of Space," *Proceedings of the IEEE*, vol. 106, no. 3, pp. 343–361, Mar. 2018, doi: 10.1109/JPROC.2018.2806218.

[8] "Global Space Economy Market: Analysis By Client Type, By Application, By Value Chain, By Region Size and Trends with Impact of COVID-19 and Forecast up to 2026," Apr. 2022. Accessed: Apr. 29, 2022. [Online]. Available: https://www.marketresearch.com/Daedal-Research-v3440/Global-Space-Economy-Client-Type-31256355/

[9] D. Housen-Couriel, "Cybersecurity threats to satellite communications: Towards a typology of state actor responses," *Article in Acta Astronautica*, 2016, doi: 10.1016/j.actaastro.2016.07.041.

[10] J. Robinson, "GOVERNANCE CHALLENGES AT THE INTERSECTION OF SPACE AND CYBERSECURITY," in *Securing Cyberspace: International and Asian Perspectives*, S. Charian and S. Munish, Eds. New Delhi: Institute for Defence Studies and Analyses, 2016, pp. 156–165. Accessed: May 05, 2022. [Online]. Available: https://www.idsa.in/system/files/book/book_securing-cyberspace_0.pdf#page=171

[11] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges," *International Journal of Information Security*, vol. 20, no. 3, pp. 287–311, Jun. 2021, doi: 10.1007/S10207-020-00503-W/FIGURES/9.

[12] M. Brian Garino and M. Jane Gibson, "Space System Threats," pp. 273–281, Accessed: May 02, 2022. [Online]. Available: https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf

[13] R. Toukebri, “Cybersecurity Risk Mitigation For Ground Systems - Space Generation Advisory Council,” Jul. 2021. Accessed: May 01, 2022. [Online]. Available: https://spacegeneration.org/cybersecurity-risk-mitigation

[14] “Challenges to Security in Space,” 2019. Accessed: May 01, 2022. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1082341.pdf

[15] S. Yusif and A. Hafeez-Baig, “A Conceptual Model for Cybersecurity Governance,” *Journal of Applied Security Research*, vol. 16, no. 4, pp. 490–513, Oct. 2021, doi: 10.1080/19361610.2021.1918995.

[16] R. de Bruin and S. H. von Solms, “Cybersecurity Governance: How can we measure it?,” *2016 IST-Africa Conference, IST-Africa 2016*, Aug. 2016, doi: 10.1109/ISTAFRICA.2016.7530578.

[17] T. Aoyama, T. Nakano, I. Koshijima, Y. Hashimoto, and K. Watanabe, “On the Complexity of Cybersecurity Exercises Proportional to Preparedness,” *Journal of Disaster Research*, vol. 12, no. 5, pp. 1081–1090, Oct. 2017, doi: 10.20965/jdr.2017.p1081.

[18] T. J. Ellis and Y. Levy, “Framework of Problem-Based Research: A Guide for Novice Researchers on the Development of a Research-Worthy Problem,” *Informing Science: the International Journal of an Emerging Transdiscipline* , vol. 11, pp. 17–33, 2008.

[19] J. S. Nye, “Nuclear Lessons for Cyber Security?,” *Strategic Studies Quarterly*, vol. 5(4), pp. 18–38, Jan. 2011.

[20] S. M. Tisdale, “CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY, KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE,” *Issues in Information Systems*, vol. 16, pp. 191–198, 2015, doi: 10.48009/3_iis_2015_191-198.

[21] D. Livingstone and P. Lewis, “Space, the Final Frontier for Cybersecurity?,” 2016.

[22] C. Baylon, “Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives,” 2014.

[23] “SATELLITE COMMUNICATIONS DOD Should Explore Options to Meet User Needs for Narrowband Capabilities Report to Congressional Committees United States Government Accountability Office,” 2021.

[24] “NASA Office of Inspector General Office of Audits NASA’S CYBERSECURITY READINESS,” 2021, Accessed: Apr. 15, 2022. [Online]. Available: https://oig.nasa.gov/hotline.html.

[25] I. Security and C. Program, “Anti-Satellite Weapons, Countermeasures, and Arms Control,” 1985.

[26] “SPACECOM chief says U.S. needs anti-satellite missile on JSTOR.” https://www.jstor.org/stable/24790160?refreqid=excelsior%3A6d7ebaa6e2a1175f779162e2a1809b74&seq=1 (accessed Apr. 15, 2022).

[27] “DoD space agency: Cyber attacks, not missiles, are the most worrisome threat to satellites - SpaceNews.” https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/ (accessed Apr. 15, 2022).

[28] “Cybersecurity Threats in Space: A Roadmap for Future Policy | Wilson Center.” https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy (accessed Apr. 15, 2022).

[29] “ENACTMENT OF TITLE 51-NATIONAL AND COMMERCIAL SPACE PROGRAMS,” 2008.

[30] L. Slapakova, T. V. Ogden, and J. Black, “Strategic and Legal Implications of Emerging Dual-Use ASAT Systems,” *NATO Legal Gazette*, no. 42, pp. 178–193, Dec. 2021, Accessed: Apr. 18, 2022. [Online]. Available: https://www.act.nato.int/application/files/5716/4032/2170/legal_gazette_42.pdf

[31] “2022 Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion,” 2022. Accessed: May 01, 2022. [Online]. Available: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

[32] “Joint Publication 3-14 ‘Space Operations,’” Oct. 2020. Accessed: May 01, 2022. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf?ver=qmkgYPyKBvsIZyrnswSMCg%3D%3D

[33] “ESA - Types of orbits.” https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits (accessed May 01, 2022).

[34] “What is a Highly Elliptically Orbit? - everything RF.” https://www.everythingrf.com/community/what-is-a-highly-elliptically-orbit (accessed May 01, 2022).

[35] M. Scholl and T. Suloway, “Introduction to Cybersecurity for Commercial Satellite Operations,” Gaithersburg, MD, Feb. 2022. doi: 10.6028/NIST.IR.8270-draft2.

[36] L. Shadbolt, “Technical Study Satellite Cyberattacks and Security,” Jul. 2021. Accessed: May 02, 2022. [Online]. Available: https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf

[37] J. Fritz, “Satellite hacking - [PDF Document],” *Culture Mandala: Bulletin of the Center for East-West Cultural and Economic Studies*, vol. 10, no. 1, pp. 21–50, Accessed: May 01, 2022. [Online]. Available: https://www.yumpu.com/en/document/read/38464408/satellite-hacking-a-guide-for-the-perplexed-international-

[38] “Satellite Jamming » Phantom Technologies.” https://phantom-technologies.com/satellite-wars/ (accessed May 01, 2022).

[39] G. Baram and O. Weschsler, “Joint Air Power Conference 2020 ‘Leveraging Emerging Technologies in Support of NATO Air & Space Power,’” 2020. Accessed: May 02, 2022. [Online]. Available: https://www.japcc.org/cyber-threats-to-space-systems/

[40] “United States Space Systems: Vulnerabilities and Threats,” Oct. 2016. Accessed: May 06, 2022. [Online]. Available: https://pubs.fas.org/_docs/10072004163734.pdf

[41] “Annual Threat Assessment of the U.S. Intelligence Community,” Feb. 2022. Accessed: May 08, 2022. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

[42] M. K. McKew, “The Gerasimov Doctrine,” *POLITICO Magazine*, Oct. 2017. Accessed: May 06, 2022. [Online]. Available: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/

[43] J. Curry and N. Drage, *The Handbook of Cyber Wargames:Wargaming the 21st Century*. 2020.

[44] N. Wilhelmson and T. Svensson, *Handbook for planning, running and evaluating information technology and cyber security exercises*. Center for Asymmetric Threat Studies (CATS), 2011. Accessed: May 08, 2022. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1235949/FULLTEXT01.pdf

[45] M. Herman, M. Frost, and Robert. Kurz, *Wargaming for leaders : strategic decision making from the battlefield to the boardroom*. McGraw-Hill, 2009.

[46] R. Beigel and J. Schuetze, “Cybersecurity Exercises for Policy Work Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work,” Apr. 2021. Accessed: May 08, 2022. [Online]. Available: https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work__0.pdf

[47] Open Textbook Library, *American government and politics in the information age.* University of Minnesota Libraries Publishing, 2016. Accessed: May 08, 2022. [Online]. Available: https://open.umn.edu/opentextbooks/textbooks/64

[48] J. G. Oakley, *Cybersecurity for Space*. Berkeley, CA: Apress, 2020. doi: 10.1007/978-1-4842-5732-6.

[49] “Presidential Policy Directive -- Critical Infrastructure Security and Resilience | whitehouse.gov.” https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed Apr. 16, 2022).

[50] G. Falco, “The vacuum of space cybersecurity,” Sep. 2018. doi: 10.2514/6.2018-5275.

[51] “ABOUT CISA | CISA.” https://www.cisa.gov/about-cisa (accessed Apr. 29, 2022).

[52] “TRENDS IN SECURITY FRAMEWORK ADOPTION A SURVEY OF IT AND SECURITY PROFESSIONALS,” 2016, Accessed: Apr. 29, 2022. [Online]. Available: www.dimensionalresearch.com

[53] “NSS2017,” *National Security Strategy of the United States of America*. The White House, Washington, D.C., 2017. Accessed: Apr. 15, 2022. [Online]. Available: https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf

[54] “National Cyber Strategy of the United States of America.” The White House, Washington, D.C., Sep. 2018. Accessed: Apr. 16, 2022. [Online]. Available: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[55] “NATIONAL SPACE POLICY UNITED STATES OF AMERICA of the D E C E M B E R 9 , 2 0 2 0”.

[56] “Executive Order on the National Space Council | The White House.” https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/01/executive-order-on-the-national-space-council/ (accessed Apr. 15, 2022).

[57] “Space Policy Directive-3, National Space Traffic Management Policy – The White House.” https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ (accessed Apr. 15, 2022).

[58] “Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House.” https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/ (accessed Apr. 15, 2022).

[59] “S.3511 - 117th Congress (2021-2022): Satellite Cybersecurity Act | Congress.gov | Library of Congress.” https://www.congress.gov/bill/117th-congress/senate-bill/3511?r=1&s=1 (accessed Apr. 16, 2022).

[60] G. C. Sen. Peters and J. Sen. Cornyn, *S.3511 - Satellite Cybersecurity Act*. Washington, D.C.: 17TH CONGRESS 2D SESSION, 2022. Accessed: Apr. 15, 2022. [Online]. Available: https://www.congress.gov/117/bills/s3511/BILLS-117s3511is.pdf

[61] N. Institute of Standards, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” 2014, doi: 10.6028/NIST.CSWP.04162018.

[62] “Small satellite sector grapples with cybersecurity requirements, cost - SpaceNews.” https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/ (accessed Apr. 16, 2022).

[63] J. Task Force, “NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations JOINT TASK FORCE”, doi: 10.6028/NIST.SP.800-53r5.

[64] “Authorities | NESDIS.” https://www.nesdis.noaa.gov/commercial-space/regulatory-affairs/licensing/authorities (accessed Apr. 16, 2022).

[65] “EXCLUSIVE: SPACECOM to unveil new commercial integration strategy this week - Breaking Defense.” https://breakingdefense.com/2022/04/exclusive-spacecom-to-unveil-new-commercial-integration-strategy-this-week/amp/ (accessed Apr. 16, 2022).

[66] “USSF Commercial SATCOM Office announces development of new security program > United States Space Force > News.” https://www.spaceforce.mil/News/Article/2230831/ussf-commercial-satcom-office-announces-development-of-new-security-program/ (accessed Apr. 16, 2022).

[67] “Commercial Satcom Providers Must Meet Federal Cyber Standards for Military - Air Force Magazine.” https://www.airforcemag.com/commercial-satellite-communications-providers-federal-cyber-standards/ (accessed Apr. 16, 2022).

[68] “(Selected) USA-series satellites,” *Colorado State University, Regional and Mesoscale Meteorology Branch*. https://rammb.cira.colostate.edu/dev/hillger/usa.htm (accessed Apr. 30, 2022).

[69] “United States Government Accountability Office MILITARY SPACE SYSTEMS DOD’s Use of Commercial Satellites to Host Defense Payloads Would Benefit from Centralizing Data Report to the Armed Services Committee, House of Representatives,” 2018.

[70] M. Nichols, “‘Semper Supra’ UNCLASSIFIED Commercial Satellite Communications Office Forecast to Industry,” 2021.

[71] “Text - H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022 | Congress.gov | Library of Congress.” https://www.congress.gov/bill/117th-congress/house-bill/2471/text (accessed Apr. 17, 2022).

[72] SmallSat Alliance, “HYBRID SPACE ARCHITECTURE Statement of Principles,” 2020. http://smallsatalliance.org/wp-content/uploads/2020/04/Hybrid-Architecture-Statement-of-Principles-v21.pdf (accessed Apr. 17, 2022).

[73] “U.S. Army Satellite Operations Brigade.” https://www.smdc.army.mil/ORGANIZATION/US-Army-Satellite-Operations-Brigade/ (accessed Apr. 30, 2022).

[74] “Warfighting Units.” https://www.spacecom.mil/About/Warfighting-Units/ (accessed Apr. 30, 2022).

[75] “Army, Navy satellite operations to consolidate under Space Force - SpaceNews.” https://spacenews.com/army-navy-satellite-operations-to-consolidate-under-space-force/ (accessed Apr. 30, 2022).

[76] “H.R.3713 - 117th Congress (2021-2022): Space Infrastructure Act | Congress.gov | Library of Congress.” https://www.congress.gov/bill/117th-congress/house-bill/3713?r=3&s=1 (accessed Apr. 16, 2022).

[77] S. S. Chopra and V. Khanna, “Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience,” *Physica A: Statistical Mechanics and its Applications*, vol. 436, pp. 865–877, Jul. 2015, doi: 10.1016/J.PHYSA.2015.05.091.

[78] O. Kodheli *et al.*, “Satellite Communications in the New Space Era: A Survey and Future Challenges”.

[79] BR, “Recommendation ITU-R M.2083-0 IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond M Series Mobile, radiodetermination, amateur and related satellite services”, Accessed: May 01, 2022. [Online]. Available: http://www.itu.int/ITU-R/go/patents/en

[80] “Enabling the connected farm – the importance of satellite communications - Inmarsat.” https://www.inmarsat.com/en/insights/enterprise/2019/enabling-the-connected-farm-the-importance-of-satellite-communications.html (accessed Apr. 30, 2022).

[81] “6 industry use cases for satellite | Eutelsat.” https://www.eutelsat.com/en/blog/6-industry-use-cases-for-satellite.html (accessed May 01, 2022).

[82] “Satellite communication: the technology behind the banking industry - axessnet.” https://axessnet.com/en/satellite-communication-the-technology-behind-the-banking-industry/ (accessed May 01, 2022).

[83] “Remote Sensing: An Overview | Earthdata,” *NASA*. https://earthdata.nasa.gov/learn/backgrounders/remote-sensing (accessed May 01, 2022).

[84] O. Dubovik *et al.*, “Grand Challenges in Satellite Remote Sensing,” *Frontiers in Remote Sensing*, vol. 0, p. 1, Feb. 2021, doi: 10.3389/FRSEN.2021.619818.

[85] T. Wellmann *et al.*, “Remote sensing in urban planning: Contributions towards ecologically sound policies?,” *Landscape and Urban Planning*, vol. 204, p. 103921, Dec. 2020, doi: 10.1016/J.LANDURBPLAN.2020.103921.

[86] L. Liu, K. M. Schaefer, A. C. Chen, A. Gusmeroli, H. A. Zebker, and T. Zhang, “Remote sensing measurements of thermokarst subsidence using InSAR,” *Journal of Geophysical Research F: Earth Surface*, vol. 120, no. 9, pp. 1935–1948, Sep. 2015, doi: 10.1002/2015JF003599.

[87] “KA-SAT Network cyber attack overview | Viasat.” https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (accessed May 08, 2022).

[88] “Viasat on Ukraine Outage: Hackers Used Misconfigured VPN to Gain Remote Access | PCMag.” https://www.pcmag.com/news/viasat-on-ukraine-outage-hackers-used-misconfigured-vpn-to-gain-remote (accessed May 08, 2022).

[89] “Viasat Reveals How Russian Hackers Knocked Thousands Of Ukrainians Offline.” https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/?sh=5403400860d6 (accessed May 08, 2022).

[90] “Viasat Satellite Hack Spills Beyond Russia–Ukraine War | WIRED.” https://www.wired.com/story/viasat-internet-hack-ukraine-russia/ (accessed May 08, 2022).

[91] “Strengthening Cybersecurity of SATCOM Network Providers and Customers | CISA.” https://www.cisa.gov/uscert/ncas/alerts/aa22-076a (accessed May 08, 2022).

[92] “EXCLUSIVE Hackers who crippled Viasat modems in Ukraine are still active-company official | Reuters.” https://www.reuters.com/business/media-telecom/exclusive-hackers-who-crippled-viasat-modems-ukraine-are-still-active-company-2022-03-30/ (accessed May 08, 2022).

[93] “SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month — and the Pentagon is taking notes.” https://www.c4isrnet.com/air/2022/04/20/spacex-shut-down-a-russian-electromagnetic-warfare-attack-in-ukraine-last-month-and-the-pentagon-is-taking-notes/ (accessed May 08, 2022).

[94] E. Mitchell *et al.*, “Jack Voltaic Critical Infrastructure and Public-Private Partnerships,” *USMA Digital Commons*, 2019, Accessed: May 09, 2022. [Online]. Available: https://digitalcommons.usmalibrary.org/aci_rp/42

[95] “Red Flag 21-1 integrates space, cyberspace for joint all-domain operations training > Air Force > Article Display.” https://www.af.mil/News/Article-Display/Article/2496993/red-flag-21-1-integrates-space-cyberspace-for-joint-all-domain-operations-train/ (accessed May 09, 2022).

[96] S. Waterman, “Cybersecurity wargame exposes space industry risks ,” Nov. 17, 2021. https://readme.security/space-cyber-wargame-exposes-satellite-industry-risks-4c18bd234d5d (accessed May 09, 2022).

[97] “Hack-s-Sat.” https://hackasat.com/ (accessed May 10, 2022).

[98] R. K. Yin, *Case Study Research: Design and Methods*, 4th ed. SAGE Publications, Inc., 2009.

[99] A. M. Riege, “Validity and reliability tests in case study research: A literature review with ‘hands-on’ applications for each research phase,” *Qualitative Market Research: An International Journal*, vol. 6, no. 2, pp. 75–86, Jun. 2003, doi: 10.1108/13522750310470055/FULL/PDF.

[100] “Cyberspace Solarium Commission,” Mar. 2020. Accessed: May 09, 2022. [Online]. Available: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Appendix 1

"Military satellite mission types in real numbers (1984-2022)"

Mission type	**Number of Satellites**
Amateur Radio	2
Communications	6
Communications intelligence	4
GPS	34
Military communications	46
Military technology	9
Military detection	12
N/A	3
Polar-orbiting weather	12
Reconnaissance	81
Space technology	3
Strategic defense	2
Technology	4
US Navy communications	2
Total:	**220**

Appendix 2

"United States Space Force Commercial Satellite Communications Office (USSF CSCO) Forecast to Industry"

Project Title & Description	Program Office / Customer	Request For Proposal (RFP)/ Projected Award / Estimated Life Cycle Value
CSS0101 BGAN Secure Terrestrial Access (BSTA) BPA Follow-On BSTA BPA providing global L-Band coverage for all branches, DoD, and Federal Agencies.	DoD	RFP November 2021 Anticipated Award February 2022 Est. Life Cycle Value $25.0 - $45.0 M
CSS0100 Consolidated BGAN & GX BPA Consolidated BGAN & GX BPA Follow-On. Follow-on contract for BGAN component of Consolidated BGAN/GX BPA for all DoD and Federal Agencies.	DoD	RFP November 2021 Anticipated Award February 2022 Est. Life Cycle Value $38.0 - $58.0 M
CTC0364 NAVAIR X-Band BPA NAVAIR X-Band BPA Follow-On. On-demand X-band bandwidth over North America to support testing and exercises. Commercial X-band Satellite Transponder Services within 250 nautical miles of Maryland to support planned MQ-4C Triton flight test.	USN	RFP November 2021 Anticipated Award March 2022 Est. Life Cycle Value $4.8 - $14.8 M
CTC0363 Program Management Unmanned Aircraft System Support Approximately 20 MHz Ku-band space segment coverage over CONUS with additional surge support possible in Alaska and Hawaii. Bandwidth will support Unmanned Aerial Vehicle (UAV) operations in the CONUS region.	USA	RFP November 2021 Anticipated Award April 2022 Est. Life Cycle Value < $10 M
CSS0104 Global X-Band BPA BPA for access to provide commercial Global X-band COMSATCOM bandwidth, teleport, terrestrial, and other ancillary services to support various customers.	DOD	RFP November 2021 Anticipated Award June 2022 Est. Life Cycle Value $114.1 - $124.1 M
CSS0106 United States Army Corps of Engineers (USACE) Satellite Service for the Deployable Tactical Operations System (DTOS) Managed network service which includes space segment for communications, Voice over Internet Protocol (VoIP), Video Tele Conference (VTC), and data communications to DTOS mobile command centers in CONUS and OCONUS.	USA	RFP December 2021 Anticipated Award April 2022 Est. Life Cycle Value < $10 M

CSS0103 Blue Force Tracker II L-band channels, SHF satellite connectivity, internet service desk, rack hosting and hands-on support services at each satellite earth station, and Host Nation Agreement services.	USA	RFP December 2021 Anticipated Award June 2022 Est. Life Cycle Value: $645 - $655 M
XXXXXXX USCENTCOM SWA AOR COMSATCOM Support (Follow-on to CTC0280) Provide 144 MHz of non-preemptible commercial Ku bandwidth for USCENTCOM.	USCENTCOM	RFP December 2021 Anticipated Award July 2022 Est. Life Cycle Value $28.2 - $38.2 M
XXXXXXX Navy Broad Area Maritime Surveillance Demonstrator (BAMS-D) Approximately 30 MHz of non-preemptible, commercial Kuband satellite bandwidth for use by NAVCENT BAMS-D Unmanned Aerial Vehicle (UAV) support. An additional 10 MHz will be provided upon request as an optional CLIN. The Government will require coverage of the Atlantic Ocean Region no more than four times in each period of performance for a duration of 2 weeks each time coverage is requested. Dates to be determined.	USN	RFP December 2021 Anticipated Award July 2022 Est. Life Cycle Value $5 - $15 M
CSS0108 Defense Coordinating Element – Hawaii Ku-band 56 kbps full duplex link within the coverage area of the Hawaiian Islands, Micronesia, Marshall Islands, Guam, Saipan, American Samoa, and the West Coast of CONUS (California, Oregon, and Washington). Internet access and VoIP service at a teleport within the area of responsibility is also required.	USA	RFP February 2022 Anticipated Award July 2022 Est. Life Cycle Value < $10 M
XXXXXXXX Proliferated LEO (PLEO) SATCOM Services Multiple Award IDIQ for PLEO satellite low-latency services, equipment and capabilities for all domains and use cases, to include both user-to-user capabilities and reach-back capabilities such as terrestrial back haul for end-to-end connectivity.	DoD	RFP March 2022 Anticipated Award August 2022 Est. Life Cycle Value $865 - $875 M Note: USSF SSC will be the contracting office

XXXXXXX Aero BPA Airborne Inmarsat Broadband and GX services for DoD and Federal Agencies. Continuation of CSS0074. Includes ancillary services for USAF/USN.	DoD	RFP March 2022 Anticipated Award August 2022 Est. Life Cycle Value $240 - $250 M
XXXXXXX Inmarsat Maritime Services BPA MSS Maritime BPA providing global L-band and GX services for all branches, DoD, and federal agencies.	DoD	RFP April 2022 Anticipated Award September 2022 Est. Life Cycle Value $27.4 - $37.4 M
CSS0107 Enterprise High Throughput Satellite Services (MEO) BPA for Global HTS managed services to include capacity and broadband, gateway, and monitoring and control of services as well as satellite terminals, field service representatives (FSR) support, training, and terrestrial backhaul.	DoD	RFP April 2022 Anticipated Award September 2022 Est. Life Cycle Value $511 - $521 M
XXXXXXX USCENTCOM COMSATCOM 288 MHz Ku-band capacity supporting USCENTCOM AOR, minimum of Afghanistan, Bahrain, Kuwait, Qatar, and United Arab Emirates in their entirety. Supports USCENTCOM's SWA network architecture and contingency mission requirements.	USCENTCOM	RFP April 2022 Anticipated Award December 2022 Est. Life Cycle Value $21.5 - $31.5 M
XXXXXXX Defense Logistics Agency (DLA) COMSATCOM Services Provides managed service support for the US (8,192 kbps x 4,096 kbps), Germany (4x exercise annually 4,096 kbps x 4,096 kbps) and Korea (4x exercise annually 4,096 kbps x 4,096 kbps). Supports DLA global defense readiness through logistics information and field support to globally deployed terminals and operators. Ability to surge globally as required.	DLA	RFP May 2022 Anticipated Award December 2022 Est. Life Cycle Value < $10 M

XXXXXXX Assistant Secretary of the Air Force for Acquisition (SAF/AQ) Bandwidth Service 1.47 MHz of Ku bandwidth supporting throughput, teleport, and terrestrial service in the Europe, the Middle East and Africa regions.	USAF	RFP May 2022 Anticipated Award December 2022 Est. Life Cycle Value < $10 M
XXXXXXX USCENTCOM SWA AOR COMSATCOM Support (Follow-on to CTC0283) 314.6 MHz Ku-band capacity supporting USCENTCOM AOR, minimum of Bahrain, Iraq, Kuwait, Oman, Qatar, Saudi Arabia, Syria, United Arab Emirates, Germany, Egypt, and portions of Libya north of 27 degrees North latitude. Supports USCENTCOM's SWA network architecture and contingency mission requirements.	USCENTCOM	RFP May 2022 Anticipated Award December 2022 Est. Life Cycle Value $72.5 - $82.5 M
XXXXXXX United States Army's Space and Missile Defense Command (USASMDC) 20 MHz of commercial C-band satellite bandwidth with global beam coverage of the following areas: Pacific Ocean Region; Kauai and Wahiawa, Hawaii; Camp Roberts, California; Sand Point, Alaska; Reagan Test Site in Kwajalein and Fort Buckner, Okinawa, Japan.	USA	RFP May 2022 Anticipated Award December 2022 Est. Life Cycle Value $2.5 - $12.5 M
XXXXXXX Army North Non-preemptible continuous Ku-band satellite bandwidth for use during exercise, day-to-day, and contingency operations to include teleport services, VoIP services, commercial Internet access, a terrestrial network backhaul from the teleports to fixed locations across the United States, and network and operational support.	USA	RFP October 2022 Anticipated Award April 2023 Est. Life Cycle Value $1.4 - $11.4 M

Appendix 3

Sample Interview questions

1. Are you regularly using any cybersecurity related standards/guidance/policies in your daily work?
2. In general, do you think cybersecurity field is regulated enough?
3. In your opinion, the cyber threat actors to traditional networks are the same or different from cyber threat actors to space systems?
4. Do you know of any non-classified cyber exercises that include space/satellite scenarios (other than Locked Shields)?
5. Do you think cyber exercises can be used as tools for informing cyber policies/regulations?
6. In your opinion, what are the goals of any cyber exercise? Or what is the one most important goal?
7. From your experience of managing and participating in cyber exercise what is the most valuable insight you were able to take away?
8. In your experience, how do different organizations implement lessons learned from cyber exercises?
9. What is the most significant shift in cyber policies or procedures that came out of a cyber exercise (that you are aware of)?

Appendix 4

Survey

Cybersecurity for Commercial Satellites

Thank you for participating in data collection activity!

This survey is a part of the research process for master level thesis on "Cybersecurity Policy for Commercial Satellite Industry" at the Tallinn University of Technology.

As commercial companies become vital participants of the "new space economy", governments need to pay more attention to cybersecurity posture of those private entities.

The goal of the thesis is threefold. First - to identify gaps in existing satellite cyber regulations. Second - to describe cyber threats to space systems. Third - to evaluate cyber exercises as a tool for CS policy making for commercial satellites.

The survey incorporates 21 questions on cybersecurity regulations, cyber risks to satellites and the role cyber exercises can play to improve policy regulations for commercial satellite industry.

Your participation and response to the best of your knowledge is highly appreciated!

What best describes your professional affiliation? *

- ◯ Private sector
- ◯ National Space Agency
- ◯ Government sector
- ◯ International Organization
- ◯ Consulting
- ◯ Research institution (not University)
- ◯ University (including research centers within University)
- ◯ Independent security researcher
- ◯ Independent policy analyst/researcher
- ◯ Other: _____

What county or countries do you work in? *

Your answer

Are you working in space related industry? *

- ◉ Yes
- ◯ No
- ◯ Other: _____

Are you working in cybersecurity related field? *

- ○ Yes
- ○ No
- ○ Other: _____

What are the cybersecurity strategies/policies/standards/regulations you are aware of? It does not have to be specific to one country. List all that you know/heard of. *

Your answer

Are you regularly using any cybersecurity related standards/guidance/policies in your daily work? *

Your answer

In general, do you think cybersecurity field is regulated enough? *

- ○ Yes. Cybersecurity sector is overregulated and does not require more standardization/compliance measures.
- ○ No. Cybersecurity sector is underregulated and more standards and regulations are required.
- ◉ Depends on the industry. Some industries need more cyber regulations then others.
- ○ Other: _____

In your opinion, please indicate the state of cybersecurity (CS) regulations in each industry. *

	Regulated sufficiently. Enough CS regulations and standards exists.	Over regulated. Difficult and costly to keep up with all CS requirements	Under regulated. Few CS regulations cause more harm than good
Communications	○	○	○
Car manufacturing	○	○	○
Healthcare	○	○	○
Banking and Financial services	○	○	○
Energy	○	○	○
Nuclear Energy	○	○	○
Defense Sector	○	○	○
Transportation	○	○	○
Space and satellites	○	○	○
Water	○	○	○
IT and software development	○	○	○

Please assess the following statements on Cybersecurity (CS) policies and regulations *

	Strongly agree	Agree	Neutral (neither agree nor disagree)	Do not agree	Strongly disagree
More CS regulations make industries and products LESS secure.	○	○	○	○	○
More CS regulations make industries and products MORE secure.	○	○	○	○	○
It is difficult to find a good balance but generally MORE regulations is better then LESS.	○	◉	○	○	○
It is difficult to find a good balance but generally LESS regulations is better then MORE.	○	○	○	○	○

Please rate your level of familiarity with cybersecurity policies and regulations for satellites or space systems? *

	1	2	3	4	5	
Somewhat familiar. Aware of its existence	○	○	○	○	○	High level of familiarity through regular professional engagements

Please rate your level of familiarity with cybersecurity risks to satellites or space systems? *

	1	2	3	4	5	
Somewhat familiar through reading or other theoretical means	○	○	○	○	○	High level of familiarity through regular professional engagements

Please rate the impact of a medium severity cyber attack on each segment to the overall security and functionality of satellite. (Let's not consider a zero day) *

	Low impact. Reversible consequences. Can be fixed quickly.	General impact. Reversible consequences. Can be fixed.	Significant impact. Reversible consequences. Fixing will take some time. Out of service temporarily.	High impact. Somewhat reversible consequences. Can be fixed but not suitable for classified or highly sensitive missions.	Severe impact. Irreversible consequences. Satellite can not be used or repaired.
Ground segment	○	○	○	○	○
Link segment	○	○	○	○	○
Space segment	○	○	○	○	○
User segment	○	○	○	○	○

Please rate vulnerability risk level of satellite development/deployment stages *

	Low risk	General risk	Significant risk	High risk	Severe risk
Manufacturing of satellites (hardware)	○	○	○	○	○
Satellite software development	○	○	○	○	○
Deployment of satellites	○	○	○	○	○
Operation of satellites	○	○	○	○	○

In your opinion, please rate the most dangerous cyber actors for space/satellite systems.

	Not a serious cyber threat in space	Equal threat capacity as in regular cyber warfare	More dangerous in space than on Earth	Less dangerous in space than on Earth	Extremely dangerous in space. Well above regular cyber warfare on Earth.
China	○	○	○	○	○
Iran	○	○	○	○	○
Russia	○	○	○	○	○
North Korea	○	○	○	○	○
Vietnam	○	○	○	○	○
Lone Hacker	○	○	○	○	○
Hacktivists	○	○	○	○	○
Script kiddies	○	○	○	○	○
Non-state organized cyber gangs	○	○	○	○	○

Please list any other threat actors to satellites and space systems that were not mentioned above.

Your answer

Have you ever participated in a cyber exercises? *

- ○ Yes
- ○ No
- ○ Other:

Are you aware of non-classified cyber exercises that include space/satellite scenarios? If yes, please list those exercises. *

Your answer

Do you think cyber exercises can be used as tools for informing cyber policies/regulations? Please elaborate why yes or no and how? *

Your answer

In your opinion, what are the goals of any cyber exercise? Or what is the one most important goal? *

Your answer

If you ever participated in a cyber exercise what is the most valuable insight you were able to take away? *

Your answer

In your experience, does the organization implement lessons learned from a cyber exercise? *

- ○ Organization conducts careful after action evaluation, develops and implements all recommendations.
- ○ Organization conducts after action review/analysis and implements some of recommendations.
- ○ Organization conducts after action review but does not implement any findings/recommendations.
- ○ No after action review is done. Organization does not need cyber exercises to know what is wrong with its cyber posture.
- ○ Cyber exercises do not impact future operations of organization.
- ○ Organization does not see a need to take part in cyber exercises.
- ○ Do not know what happens in the organization after a cyber exercise.
- ○ Other:

Any comments or feedback is welcome!

Your answer

Non-Exclusive License for Publication and Reproduction of Graduation Thesis

Plain license for allowing the thesis to be available and reproducible for the public

I, Olena Roraff

1. Allow the Tallinn University of Technology without any charges (Plain license) my work

”*Cybersecurity Policy For The Satellite Industry: Governance Challenges and Solutions*”

supervised by Eric Jackson,

1.1. to be reproduced for the purpose of conservation and electronic publication, including the digital repository of the Tallinn University of Technology, until the end of copyrighted time limit;
1.2. to be available to the public through the Tallinn University of Technology online environment, including the digital repository of the Tallinn University of Technology, until the end of the copyrighted time limit.

2. I am aware, that all rights, named in section 1, will remain to the author.

3. I confirm that by allowing the use of the Plain licence, no intellectual rights of third parties will be violated as set in the personal data protection act and other legislation.

signed by Olena Roraff

May 09 2022