# A Collaborative Cybersecurity Training Policy for Future Space Endeavors

**Chelsea H. Wright**

*Information Security and Intelligence, Ferris State University, United States of America*

## ABSTRACT

The Bureau of Labor Statistics states that information security analysts are projected to have a 35% growth rate between 2021-2031. (Fastest growing occupations: Occupational outlook handbook 2022) With the growing use of space for technology in both the government and commercial sectors, there becomes a need for training that is specific to space cybersecurity. The United States government relies on the ability of commercial satellites to be accessed and operate in space which helps with the advancement of security, economic prosperity, increased knowledge, and scientific knowledge for the Nation (Scholl, 2021). This is more prevalent in space, as in accordance with The Outer Space Treaty, "space activities are for the benefit of all nations, and any country is free to explore orbit and beyond" as well as "There is no claim for sovereignty in space; no nation can "own" space, the Moon or any other body." (International Space Law 2021).

Much of the world's technology activity is reliant on assets that are space-based and infrastructure, this infrastructure is vulnerable to cyberattacks. If the technological infrastructures in space are insecure this will impede economic development and create increased risks to communications, transportation, financial transactions, energy, agriculture, food, weather monitoring, and defense (Livingstone & Lewis, 2016). A strong training program focused on cybersecurity, space situational awareness, and space domain awareness for future space endeavors is critical.

This study will investigate what current training policies are being utilized for space cybersecurity and frameworks. This research looks to answer if a common global framework for space cybersecurity training can be established from known cybersecurity frameworks to be used in space cybersecurity.

Aerospace outlines five specific cybersecurity principles that the Space policy Directive-5 (SPD-5) defines for space policies. These policies are used as the groundwork for the United States government method, which also includes working with the space industry that is in the commercial sector that will help outline the best practices, develop cybersecurity norms, and advocate for improved cybersecurity behaviors (Bailey, 2020). These policies and standards are compared to the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework is created based on known effective practices using five key Functions; Identity, Protect, Detect, Respond, and Recover (Mahn et al., 2021). Using a solid foundation of well-known cybersecurity practices to help define a basis for a space cybersecurity framework and policy to be used for training is part of what defined this research. This study analyzes current security training practices for space endeavors, both terrestrially and within space. From this research, a new training policy framework for space cybersecurity will be created that can be utilized for training programs to reference.

## 1. INTRODUCTION

The space domain is one of the newest sectors to venture into the need for cybersecurity. Like technology throughout the globe, the space realm needs to be heavily secured. The citizens of the world rely heavily on the use of space technology; satellites for phone connection and signal, weather warnings, observations, and predictions, autonomous vehicle management, internet connection, government security, etc. (*Why we need increased cybersecurity for space-based services,*2022). The increased use of technology in space indicates the need for properly trained individuals in space cybersecurity. This study analyzed cybersecurity training programs that have training for civilians to participate in that focused on

cybersecurity in space and compared their programs to the NIST Cybersecurity Framework's Key Functions.

The ability of commercial satellites to access and operate in space is critical to the U.S. government to help with economic prosperity, the advancement of security, and increase scientific knowledge for the Nation. (Scholl, 2021) Space is being used by both governmental entities worldwide as well as commercially. There are risks and challenges to maintaining a secure information systems platform in space, both terrestrially and within space.

## 2. MATERIALS AND METHODS

This study used qualitative research empirical study, and content analysis methodology to analyze space cybersecurity training programs. Through intense searches using library databases of Google Scholar (*Google Scholar*) search engine and the Association for Computing Machinery (ACM) database (*ACM Digital Library* 2023) these unclassified programs for ease of civilian participation were selected to be used for this research based on their ease of findability, trusted credentials and endorsements which are listed in the "Brief Overview of the Training Program Entities" section. Content analysis methodology (Cavanagh, 1997) was used to determine similarities and theoretical understanding of the topics listed in the training programs. Capitol Technology University (CapTech), Tonex, the American Institute of Aeronautics and Astronautics (AIAA), and Ferris State University space cybersecurity programs were used in this empirical study.

### *Data Sources*

Sources easily findable and accessible for civilians were considered for this study using library databases within Google Scholar (*Google Scholar*) and Ferris State University access to the Association for Computing Machinery (ACM) database (*ACM Digital Library* 2023).

Information about the training programs and their coursework/objectives was collected through extensive online database research of each program's online database. Coursework and objectives were defined on each training program's website and are outlined within this study. Capitol Technology University's website for Doctor of Philosophy (Ph.D.) in Space Cybersecurity. (*Doctor of Philosophy (PhD) in Space Cybersecurity* 2023). Tonex's website entitled *Certified Space Security Specialist Professional (CSSSP)* (*Certified Space Security Specialist Professional (CSSSP)* 2023). The American Institute of Aeronautics and Astronautics website for Events & Learning (*Understanding cybersecurity in the space domain - online short course (Oct 16-19, 2023)* 2023). Ferris State University *Information security and intelligence* website (*Information security and intelligence (MS)* 2022).

### *Study Progression*

As the research progressed the four entities' space cybersecurity training programs were thoroughly stated, outlining the coursework/objectives as stated by the program's online databases. The research investigated what the National Institute of Standards and Technology (NIST) states are the five key functions of the Cybersecurity Framework. This laid the groundwork to compare what these four training programs' coursework and objectives are educating and what functions they fall under within the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework key functions were used to create a chart for each training program to highlight each specific course/objective and which key function it could fall under. This was acquired and created for each of the four training programs as separate charts.

After an assessment of the NIST and the different entities comparison, research into what is specifically needed for cybersecurity in the space domain was evaluated by reviewing The Space Policy Directive-5 produced by the White House. This policy directive outlines specific principles that should be followed for space cybersecurity.

The research design (Fig. 1) began with an empirical literature review utilizing Google Scholar and The Association for Computing Machinery Database. An analysis of cybersecurity controls and areas of focus in the space domain consisted of utilizing content analysis methodology to determine NIST CSF commonalities combined with the United States Space Policy Directive –5, and the (N=4) unclassified, accessible, civilian training programs. This process developed a Framework Function Chart to visually process the research. Using manual Natural Language Processing, commonalities, and gaps were identified and added to the Framework Function Charts. The result was a Framework Function Chart visually identifying commonalities among the (N = 4) training programs, NIST CSF, and United Space Policy Directive –5 topics.

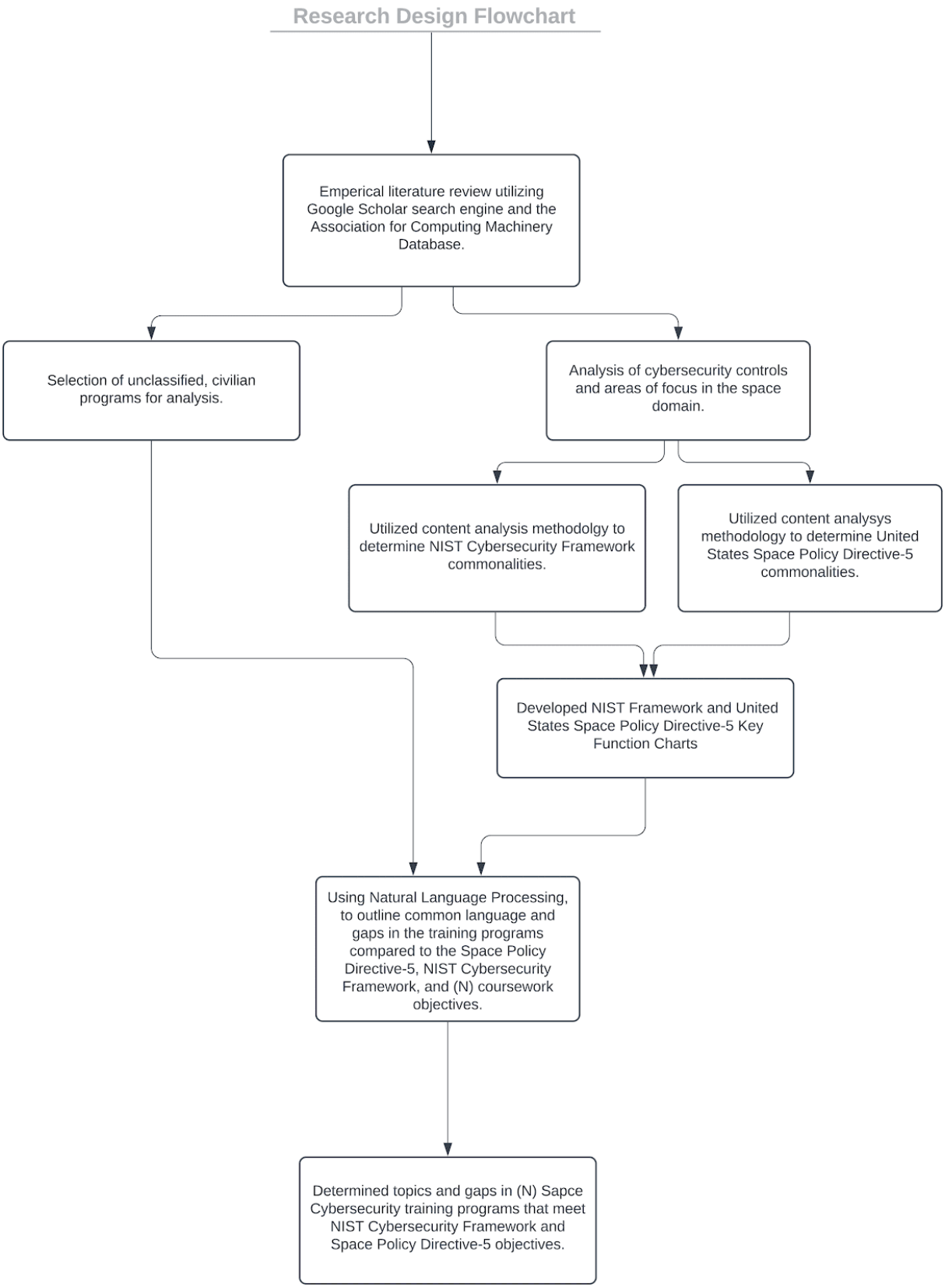

Fig. 1 The Research Design Flowchart highlighting the study progression from literature review through the selection of programs to be studied and the analysis process of the NIST Cybersecurity Framework as well as the Space Policy Directive-5 to arrive at an outcome using Natural Language Processing to analyze gaps in the training programs.

*Brief Overview of the Training Program Entities* (N=4)

> *Capitol Technology University* - A private not-for-profit University whose mission is "To educate individuals for professional opportunities in engineering, computer and information sciences, and business. We provide relevant learning experiences that lead to success in the evolving global community." (*At a glance*). The State of Maryland authorizes Capitol Technology University to confer a Doctor of Philosophy (Ph.D.) degree in Cybersecurity. (*Accreditation* 2023). Capitol Technology University has been designated by the National Security Agency and Department of Defense as a National Center of Academic Excellence in Cyber Defense. (*Doctor of Philosophy (Ph.D.) in Space Cybersecurity* 2023).
>
> *Tonex* - A company that specializes in training, seminars, courses, and consulting services. The mission of the company is to help organizations succeed. They work with large and small companies to offer courses relevant to the latest technology, business trends, and important subject matter. (*About Us* 2022). Tonex has a client page that showcases who their clients are which include the NSA, NASA, U.S. Air Force, U.S. Department of Treasury, U.S. Army, U.S. Marine, U.S. Navy, and more noteworthy government agencies as well as Fortune 500 companies. (*Tonex clients* 2023).
>
> *American Institute of Aeronautics and Astronautics (AIAA)* - AIAA is a technical society that is committed to the aerospace profession globally. Their purpose is "to ignite and celebrate aerospace ingenuity and collaboration, and its importance to our way of life." (*About the American Institute of Aeronautics and Astronautics (AIAA)*). "AIAA leads the way on issue advocacy that impacts the Aerospace sector. The Institute delivers extensive technical expertise and policy guidance to decision-makers at the federal and state levels, serving as a reliable resource on a full spectrum of aerospace issues." (*An Advocacy for Aerospace*).

*Ferris State University* - A four-year public university with a mission that "prepares students for successful careers, responsible citizenship, and lifelong learning. Through its many partnerships and its career-oriented, broad-based education, Ferris serves our rapidly changing global economy and society." (*Mission, vision, and Core Values*). Ferris State University Information Security and Intelligence (ISI) programs are accredited as a Center of Excellence in all Information Assurance subject areas by the NSA. Ferris has been designated as a National Center for Digital Forensic Academic Excellence by the Department of Defense Cyber Command and the Air Force Office of Special Investigations. Ferris has also been deemed a Center of Academic Excellence in Cyber Defense by the NSA and the Department of Homeland Security. (*Information security and intelligence (MS)* 2022).

*Brief Overview of National Institute of Standards and Technology Cybersecurity Framework*

There are five key functions for the Framework for Cybersecurity based on the NIST (Fig 2). "Created through collaboration between industry and government, the Cybersecurity Framework seeks to promote the protection of critical infrastructure." (Marron et al., 2019).

I. Identify
   a. Create an overall comprehension that will manage cybersecurity risk to data, assets, systems, and capabilities. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022).

II. Protect
   a. Create and implement suitable safeguards to make certain of the delivery of services. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022).

III. Detect

a. Create and implement suitable ventures to identify the occurrence of an event in cybersecurity. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022).

IV. Respond

a. Create and implement suitable ventures to take action regarding detecting cybersecurity events. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022).

V. Recover

Create and implement suitable ventures to sustain plans for resilience and to re-establish any services or capabilities that were hindered due to a cybersecurity event. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022).

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

Fig. 2. NIST Five Key Functions for the Framework for Cybersecurity. (Taken from the NIST Technical Note 2051: *Cybersecurity Framework Smart Grid Profile*). This image is used to compare the training program's coursework.

*Brief Overview of Space Cybersecurity Domain Principles - Space Policy Directive - 5*

Critical aspects of the practices and principles for cybersecurity that are important to terrestrial systems have certain practices that should be considered heavily when applied to cybersecurity within the space domain. Due to the nature of space vehicles and their location, remote access is crucial to being able to perform updates and remotely respond to incidents, therefore designing these vehicles with this notion in mind is critical. (*Cybersecurity Principles for Space Systems* 2020).

The Space Policy Directive-5 describes the space systems cybersecurity principles to be followed.

**"Sec. 4**. *Principles.* (a) Space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering. Space systems should be developed to continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations. Space system configurations should be resourced and actively managed to achieve and maintain an effective and resilient cyber survivability posture throughout the space system lifecycle.
(b) Space system owners and operators should develop and implement cybersecurity plans for their space systems that incorporate capabilities to ensure operators or automated control center systems can retain or recover positive control of space vehicles. These plans should also ensure the ability to verify the integrity, confidentiality, and availability of critical functions and the missions, services, and data they enable and provide. At a minimum, space system owners and operators should consider, based on risk assessment and tolerance, incorporating in their plans:
(i) Protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime;
(ii) Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;
(iii) Protection against communications jamming and spoofing, such as signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime;
(iv) Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including insider threats. Such practices include logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training inclusive of insider threat mitigation precautions;
(v) Adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies; and
(vi) Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.
(c) Implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity, including through the consideration and adoption, where appropriate, of cybersecurity best practices and norms of behavior.
(d) Space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as Information Sharing and Analysis Centers to the greatest extent possible, consistent with applicable law.
(e) Security measures should be designed to be effective while permitting space system owners and operators to manage appropriate risk tolerances and minimize undue burden, consistent with specific mission requirements, United States national security and national critical functions, space vehicle size, mission duration, maneuverability, and any applicable orbital regimes."
(*Cybersecurity Principles for Space Systems* 2020).

## 3. RESULTS

***Key Function Charts - Comparison Chart of Program Coursework and NIST Key Functions***

Below are comparison charts of the NIST Cybersecurity Framework Key Functions vs the training programs and if they fall into one or more of the NIST key functions for cybersecurity. By comparing the definition for each key and looking at the known objectives or specifics of each course/coursework, a value was given on how quantifiably the course would seem to meet the requirements for one or more of the NIST Cybersecurity key functions.

Using quantifiable data for qualitative research, a scale (Fig. 3) was produced to categorize the coursework into a rating of how well the coursework was defined within the NIST Cybersecurity Framework key functions.

| Key | Value |
|---|---|
| 1 | No mention or direct correlation with the NIST Cybersecurity Framework key function. |
| 2 | Minimal course focus on the NIST Cybersecurity Framework key function. |
| 3 | Moderate focus on the NIST Cybersecurity Framework key function. |
| 4 | Defined focus on the NIST Cyber-security Framework key function. |
| 5 | Strongly defined focus on the NIST Cybersecurity Framework key function. |
| ? | Unclear, the research/objectives could or could not be focused on the NIST Cybersecurity Framework |

Fig. 3 The Key scale used to define quantifiable value for qualitative results. This is to be referenced for the following training program's Key Function Charts.

*Capitol Technology University (Fig. 4).*

| | | NIST Framework Key Function | | | | |
|---|---|---|---|---|---|---|
| | | Identify | Protect | Detect | Respond | Recover |
| Capitol Tech Course Name | Space Cybersecurity Research Background | 3 | 3 | 4 | 4 | 4 |
| | Space Cybersecurity Research Methodologies | 4 | 5 | 3 | 2 | ? |
| | Space Cybersecurity Future Demands | 2 | ? | ? | 3 | 3 |
| | Strategies for Space Cybersecurity | 3 | 3 | 3 | 3 | 3 |
| | Space Cybersecurity Research Proposal | 2 | ? | ? | 4 | 4 |

Fig. 4. Capitol Technology University's coursework identifying which key function each course categorizes within. Due to the nature of this program being subjective on account of the student's path of research for their Ph.D. Ph.D. coursework, question marks were placed beside key functions).

*Tonex (Fig. 5).*

| | | NIST Framework Key Function | | | | |
|---|---|---|---|---|---|---|
| | | Identify | Protect | Detect | Respond | Recover |
| Tonex Course Names | CSSSP Level 1 Coursework | 5 | 5 | 1 | 2 | 2 |
| | CSSSP Level 2 Coursework | 5 | 5 | 5 | 5 | 5 |
| | CSSSP Level 3 Coursework | 3 | 3 | 3 | 4 | 4 |

Fig. 5. Tonex coursework identifying which key function each course categorizes within.

*AIAA (Fig. 6).*

| AIAA Tech Course Name | NIST Framework Key Function | | | | |
|---|---|---|---|---|---|
| | Identify | Protect | Detect | Respond | Recover |
| Understanding the overall challenges of cybersecurity within space organized by the SpaDoCs Framework | ? | ? | ? | ? | ? |
| Understand and define major objectives of cybersecurity (CIA Triad) | 5 | 5 | 1 | 1 | 1 |
| Recognize cyber vulnerabilities and threats of missions in space and space systems | 5 | 2 | 2 | 2 | 1 |
| Distinguish between the different layers within the space domain and the compromising elements | 1 | 1 | 1 | 1 | 1 |
| Use cybersecurity principles and apply them within the space domain in terms of vulnerabilities and threats | 5 | 2 | 2 | 2 | 1 |
| Analyze the vulnerabilities and threats and what the attack vectors are for different space domain scenarios. | 3 | 2 | 4 | 3 | 2 |

Fig. 6. AIAA coursework identifying which key function each course categorizes within.

*Ferris State University (Fig. 7).*

| Ferris Course Names | NIST Framework Key Function | | | | |
|---|---|---|---|---|---|
| | Identify | Protect | Detect | Respond | Recover |
| Space Operations | 5 | 5 | 1 | 1 | 1 |
| Space Communications | 3 | 4 | 1 | 2 | 2 |
| Space Technology and Cybersecurity | 3 | 5 | 5 | 5 | 3 |

Fig. 7. Ferris State University coursework identifying which key function each course categorizes within.

These quantified results were combined and a total for each NIST Key Function (Fig. 8) was articulated showing that these training programs' coursework/objectives focus strongly on the Key Function of Identifying and the least on Detection.

| | NIST Framework Key Function | | | | |
|---|---|---|---|---|---|
| | Identify | Protect | Detect | Respond | Recover |
| Key/Value Total | 57 | 40 | 36 | 44 | 37 |

Fig. 8. The total combined values of each training program's coursework/objectives and the NIST Cybersecurity Framework Key Function.

The purpose of this study was to examine different space cybersecurity training programs that are currently available and see how they compare to the NIST standard Cybersecurity Framework, while also keeping in mind the specific needs of space. Gaps in training were also identified, based on the information provided.

***Training Programs Comparison***

*University Comparison*

Capitol Technology University and Ferris State University have (or are soon to have for Ferris) graduate programs that are specific to Space Cybersecurity. To compare these programs based on their coursework and what they fall into within the NIST Cybersecurity Framework Key Functions it shows that both programs have different coursework that falls within the different categories of the NIST Framework.

Capitol Tech's program is a full doctorate, and the basis of the program is research that is tailored to the individual student's preference. This creates a caveat in understanding if the training for the graduate degree is fully expected to train/teach students about all entities of cybersecurity in space as it pertains to the NIST Cybersecurity Framework Key Functions. According to Capitol Tech's Doctoral Program Requirements, "All students interested in applying for a doctoral degree need a master's degree in a relevant field, a resume showing a minimum of 5 years of directly related work experience plus 2 completed recommendation forms." (*Doctoral admissions* 2023). All students applying for the Ph.D. in Space Cybersecurity are required to have a master's degree in cybersecurity or a type of computer technical degree with a working knowledge of at least 5 years that is relevant to security. Based on this information it is to be assumed these students understand the NIST Framework's key elements; Identify, Protect, Detect, Respond, and Recover. As this doctorate is heavily based on the individual student's research it was harder to determine the gaps in training.

Ferris State University's upcoming Graduate Certificate in Space Cybersecurity gives an overall picture of cybersecurity within the space domain. The coursework lays a solid foundation for the particulars of space operations, space communications, space technology, and cybersecurity. By training on the operations in space and moving into the communications used, and then introducing the technology used in space and the cybersecurity it takes to secure the space domain, Ferris gives a robust understanding of what the NIST Cybersecurity Framework lays out for cybersecurity and applies it to space.

A gap in training that was not evident in the coursework listed is referenced within the Space Policy Directive-5, section (b) (vi) which states, “Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.” (*Cybersecurity Principles for Space Systems* 2020). While Ferris’s curriculum does highlight Space Operations, it does not define risk analysis of supply chain risks. This element of the Space Policy Directive could fall under Ferris’s “Incidence Response for Space Systems.”

*Non-University Comparison*

Tonex starts with courses taught over 4 days for each level. Level 1 of the courses is geared towards the basics of what is essential for security in space and the prevention, defense, and maintenance while also analyzing the vulnerabilities of assets in space. This first level of coursework seems to fall heavily within the NIST Framework’s first two key functions; identify and protect.

The next level of courses is another 4-day training for Level 2. This coursework expands into multiple elements within space including; technical security operations, planning, vulnerability management, forensics, threats, and malware analysis. This coursework seems to fall heavily under all of the NIST Framework’s Cybersecurity categories.

The third level of courses is another training consisting of 4 days for Level 3. This coursework trains on the defensive and offensive operations in space cybersecurity which would seem to fall under the NIST Cybersecurity Framework’s key functions of response and recovery.

Tonex has a thorough training program for space cybersecurity, this is especially noticeable in the coursework that applies to the Level 2 CSSSP training. There is a possible gap identified that relates to the Space Policy Directive’s section (b) (ii) which states, “Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;” (*Cybersecurity Principles for Space Systems* 2020). The physical security of space vehicles is not defined within the curriculum of training.

AIAA is a short course offered online as a 4-day program that has 5-hour classes. While the coursework states it is designed around the SpaDoCs Framework, this was not a framework that has easily accessible information on it. Due to this, the comparison with the NIST Cybersecurity Framework is used for this analysis as well. The coursework defined states they look to train on understanding cybersecurity in space, recognizing the vulnerabilities and compromising elements, and analyzing and applying cybersecurity principles to these threats. The different courses fall under the different NIST Framework key functions depending on what is being taught, the strongest key function being Identify.

The AIAA short course does not specifically articulate that it discusses risk management like the Space Policy Directive-5, section (b) (vi) states, “Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.” (*Cybersecurity Principles for Space Systems* 2020).

Understanding the threats and analyzing the risks within the supply chain for space vehicles should be considered for training in space cybersecurity programs.

***Overall Assessment***

For students looking to receive a degree or graduate certification in space cybersecurity, both Capitol Technology University’s Doctor of Philosophy (Ph.D.) in Space Cybersecurity and Ferris State University’s graduate certification in Space Cybersecurity offers a well-defined NIST-based program. For students who do not already have a background in cybersecurity and a working background in IT of a

minimum of 5 years, Ferris State University offers a program that touches on the evolving aspects of space cybersecurity, and their coursework on Space Technology and Cybersecurity includes all of the five key functions of the NIST Cybersecurity Framework.

For those individuals who may not be looking for a degree or graduate certification but still want to understand cybersecurity in the space domain, both Tonex and the American Institute of Aeronautics and Astronautics offer short courses that dive into why cybersecurity in space is so important. Their courses touch on multiple key functions of the NIST Cybersecurity Framework. Tonex courses help prepare individuals to take the International Society of Space Security Specialists IS$^4$ certification exam. The CSSSP certification is a highly respected certification within the space security industry. (*Certified Space Security Specialist Professional (CSSSP)* 2023).

## 4. DISCUSSION

Overall, unclassified space cybersecurity training programs used in this research have coursework designed for both students seeking formal higher education training within space cybersecurity and individuals seeking short courses with objectives in cybersecurity in space. Each of the space cybersecurity programs had coursework and objectives that fell within the scope of the NIST Cybersecurity Framework and when compared to the Space Policy Directive-5 specific gaps were identified that can be considered for future training programs.

1. The physical security of the space vehicles is not evident in the training coursework/objects, which is a highlighted principle of the Space Policy Directive-5 (b) (ii).
2. Coursework/objectives to discuss collaboration and communication amongst other training program entities, space authorities, and space industry leaders is the principle (d) of the Space Policy Directive-5 and is not evident within the training program's current curriculums.

*Limitations*

The coursework assessed for each training program is a high-level view of what each course entails. To assess each training program with actual course material, a complete dynamic of what is studied, and materials used would help give a more in-depth comparison of space cybersecurity training programs. The time constraint of the research was also a limitation.

Clearance to research and observe classified current government space cybersecurity training programs would create a more robust understanding of what specifics in training government entities are looking for with the future of space cybersecurity. Clearance would also allow for more search engine databases for research. This research also has a limited amount of comparable space cybersecurity training programs due to the limited availability of space cybersecurity programs in existence.

*Future Work*

For future studies, consideration of using an Artificial Intelligence tool to enhance the survey of commonalities using NLP. This would create a statistical analysis output with precise data metrics.

Acquiring Top Secret security clearance to expand the data set of training programs used for research.

A creation of surveys that are assessed by space cybersecurity industry leaders, educators, and students.

***Suggested Combined Coursework Policy for Future Space Cybersecurity Programs***

A suggested policy would have coursework that combines the strongest (Key Value 5) NIST Framework Key Functions according to the Key Value chart of all four programs and would include the following:

I. Prevention, Defense, and maintenance
II. Space Security Essentials
III. Space Asset Vulnerabilities
IV. Space Vehicles
    i. Architecture and hardware
V. Core Space Technologies
    i. Security controls, wireless, encryption
    ii. Solutions using AI
VI. Managing Technical Space Security Operations
    i. Ground stations, satellites, other space systems.
VII. Space RMF and Critical Controls
VIII. Space Planning, Policy, Leadership
IX. Space Vulnerability Management
    i. Recognizing cyber vulnerabilities and threats of missions in space.
X. Leadership Essentials
XI. Space Project Management
XII. Space Audit & Legal
XIII. Space Law & Investigations
    i. Policy, law, ethics
XIV. Space Forensics
    i. Network, Threat Intel, Battlefield
XV. Malware Analysis & Space Threat Intelligence
XVI. Space Cyber Threat Intelligence
XVII. Understanding and defining major objectives of cybersecurity (CIA Triad).
XVIII. Research methods and strategies to continuously understand space cybersecurity.
XIX. Incident Response for Space Systems
    i. Penetration testing
XX. Defensive and Offensive Space Operations
    i. Defense: Focusing on cyber defense essentials and blue teaming
    ii. Offense: Focusing on cyber defense essentials and red teaming
XXI. Focused course on consolidating, and collaborating ideas and policies with other programs.

## 5. CONCLUSION

The most common NIST Cybersecurity Framework Key Functions identified throughout the training programs was Identify. The first key function the NIST lists is to Identify. Create an overall comprehension that will manage cybersecurity risk to data, assets, systems, and capabilities. (*NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC* 2022). This is a critical training objective and a positively identified quality amongst all four of the training entities. The ability to identify cybersecurity practices in space and an overall understanding of what cybersecurity is sets a good foundation for a space cybersecurity training program.

A positive addition to these space cybersecurity training programs would be a course that focuses on commonalities, consolidating, and collaborating ideas and policies with other programs, universities, government agencies, and more with the intent of securing the space domain efficiently and effectively with others who share the same goals and passion for cybersecurity in space.

Space cybersecurity is constantly evolving just as the technology it is designed to secure is. There are a few outlined gaps in the training programs in this study. One collaborative gap throughout all four programs is highlighted in the Space Policy Directive-5, section (d) states, “Space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as Information Sharing and Analysis Centers to the greatest extent possible, consistent with applicable law.” (*Cybersecurity Principles for Space Systems* 2020).

The creation of a program that compiles the strongest coursework identified from these four studied programs and looks to bridge the gap of the weakest NIST key function of detection that would serve the Space Cybersecurity community.

## 6. REFERENCES


[1] American Institute of Aeronautics and Astronautics. (2023). *Understanding cybersecurity in the space domain - online short course (Oct 16-19, 2023)*. AIAA Shaping the Future of AeroSpace. Retrieved April 1, 2023, from https://www.aiaa.org/events-learning/courses-workshops/detail/understanding-cybersecurity-in-the-space-domain-course.

[2] American Institute of Aeronautics and Astronautics. (n.d.). *About the American Institute of Aeronautics and Astronautics (AIAA)*. About AIAA. Retrieved April 1, 2023, from https://www.aiaa.org/about.

[3] American Institute of Aeronautics and Astronautics. (n.d.). *An Advocacy for Aerospace*. Advocacy. Retrieved April 4, 2023, from https://www.aiaa.org/advocacy/.

[4] Association for Computing Machinery. (2023). ACM Digital Library. Retrieved April 15, 2023, from https://dl-acm-org.ferris.idm.oclc.org/.

[5] *At a glance*. Capitol Technology University. (n.d.). Retrieved April 1, 2023, from https://www.captechu.edu/about-capitol/at-a-glance.

[6] Bailey, B. (2020, October 15). Establishing Space Cybersecurity Policy, standards, and risk management practices: The Aerospace Corporation. Aerospace. Retrieved January 28, 2023, from https://aerospace.org/paper/establishing-space-cybersecurity-policy-standardsand-risk-management-practices.

[7] Bartlett, Maurice S. "Multivariate analysis." Supplement to the journal of the royal statistical society 9.2 (1947): 176-197.

[8] Capitol Technology University. (2023). *Accreditation*. Capitol Technology University. Retrieved April 4, 2023, from https://www.captechu.edu/about-capitol/accreditation.

[9] Capitol Technology University. (2023). *Doctor of Philosophy (PhD) in Space Cybersecurity*. Capitol Technology University. Retrieved April 1, 2023, from https://www.captechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd.

[10] Capitol Technology University. (2023). *Doctoral admissions*. Capitol Technology University. Retrieved April 6, 2023, from https://www.captechu.edu/admissions/doctoral.

[11] Cavanagh, S. (1997). Content analysis: concepts, methods and applications. *Nurse researcher*, *4*(3), 5-16.): 5-16.

[12] *Certified Space Security Specialist Professional (CSSSP)*. Tonex Training. (2023, March 31). Retrieved April 1, 2023, from https://www.tonex.com/training-courses/certified-space-security-specialist-professional-csssp/.

[13] Ferris State University. (2022). *Information security and intelligence (MS)*. Ferris State University. Retrieved April 4, 2023, from https://www.ferris.edu/business/information-security-intelligence-grad/homepage.htm.

[14] Ferris State University. (n.d.). *Mission, vision and Core Values*. Ferris State University. Retrieved April 1, 2023, from https://www.ferris.edu/administration/president/mission.html.

[15] Google. (n.d.). Google Scholar. Retrieved April 16, 2023, from https://scholar.google.com/ .

[16] International Society of Space Security Specialists. (2023, February 22). *CSSSP Level 1: Specialist*. IS4.ORG. Retrieved April 1, 2023, from https://is4.org/csssp-levels/csssp-level-1-specialist/ .

[17] Livingstone, D., & Lewis, P. (2016, September). Space, the Final Frontier for Cybersecurity? Chatham House. Retrieved January 28, 2023, from https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-spacefinal-frontier-cybersecurity-livingstone-lewis.pdf.

[18] Mahn, A., Marron, J., Quinn, S., & Topper, D. (2021). Getting started with the NIST Cybersecurity Framework: A quick start guide. *NIST Special Publication 1271*. https://doi.org/https://doi.org/10.6028/nist.sp.1271.

[19] Marron, J., Gopstein, A., Bartol, N., & Feldman, V. (2019, July). *NIST Technical Series Publications*. Cybersecurity Framework Smart Grid Profile. Retrieved April 2, 2023, from https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf.

[20] National Archives. (2020, September 10). *Cybersecurity Principles for Space Systems*. Federal Register: The Daily Journal of the United State Government. Retrieved April 2, 2023, from https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems.

[21] National Institute of Standards and Technology. (2022, April 16). *NIST Cybersecurity Framework: A quick start guide - cybersecurity framework: CSRC*. CSRC. Retrieved April 1, 2023, from https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide.

[22] Scholl, M. (2021, June 29). Introduction to Cybersecurity for Commercial Satellite Operations (2nd draft). NIST. Retrieved January 28, 2023, from https://csrc.nist.gov/publications/detail/nistir/8270/draft.

[23] Teaching Science and Technology Inc. (n.d.). *About Us*. TSTI. Retrieved April 1, 2023, from https://www.tsti.net/about-teaching-science-technology-inc/.

[24] Tonex, Inc. (2022, February 23). *About Us*. Tonex Training. Retrieved April 1, 2023, from https://www.tonex.com/about-us/.

[25] Tonex, Inc. (2023). *Certified Space Security Specialist Professional (CSSSP)*. Tonex Training. Retrieved April 6, 2023, from https://www.tonex.com/training-courses/certified-space-security-specialist-professional-csssp/.

[26] Tonex, Inc. (2023). *Tonex clients*. Tonex Training. Retrieved April 4, 2023, from https://www.tonex.com/clients/#a.

[27] U.S. Bureau of Labor Statistics. (2022, September 8). *Fastest growing occupations: Occupational outlook handbook*. U.S. Bureau of Labor Statistics. Retrieved February 27, 2023, from https://www.bls.gov/ooh/fastest-growing.html.

[28] *Why we need increased cybersecurity for space-based services*. World Economic Forum. (2022). Retrieved February 13, 2023, from https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/