Pacific Northwest
NATIONAL LABORATORY

PNNL-39723

Cyber Halo Innovation Research Program (CHIRP) Student Research Report

Program Analysis

July 2026

Penny McKenzie
Aubrie Kendall

U.S. DEPARTMENT of ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-39723

Cyber Halo Innovation Research Program (CHIRP) Student Research Report

Program Analysis

July 2026

Penny McKenzie
Aubrie Kendall

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Executive Summary

The Cyber Halo Innovation Research Program (CHIRP) conducted multi-year, mission-focused research addressing emerging cybersecurity challenges affecting space and ground systems. Students from California State University San Bernardino (CSUSB), University of Texas El Paso (UTEP), and California State University Dominguez Hills (CSUDH) conducted structured research, developed proof-of-concept demonstrations, participated in applied cybersecurity training, and collaborated with Space Systems Command (SSC), academic, and industry partners.

This report documents the research questions, methodologies, findings, demonstrations, and student contributions associated with each cohort. It also summarizes the program's workforce-development outcomes, including applied cybersecurity training, professional certifications, technical credentials, and partnerships with organizations such as CT Cubed, Inc. and ISC2. Collectively, CHIRP strengthened the space-cybersecurity workforce pipeline and produced research and prototype efforts that may inform future cybersecurity assessments, test and evaluation activities, cyber-range development, acquisition planning, operational training, and mission-assurance initiatives.

"The language in this document was edited by PNNL AI Incubator (GPT-5.6 Luna from OpenAI)for grammar, clarity, and concision. Initial drafts were created by the author and all final language was reviewed for accuracy."

Acknowledgments

The CHIRP team gratefully acknowledges Space Systems Command (SSC) S6 for its continued support, collaboration, and confidence in the program. SSC's engagement provided students with mission-relevant research topics, operational context, technical feedback, and opportunities to apply their work to space-cybersecurity challenges.

The team especially appreciates SSC's support of innovative research addressing Zero Trust, cyber-range development, artificial intelligence, post-quantum cryptography, resilient communications, space-domain awareness, and mission assurance. SSC's collaboration, mentorship, and willingness to review and consider student research and proof-of-concept demonstrations strengthened the quality and relevance of the program's outcomes.

The CHIRP team also acknowledges the contributions of its academic, industry, and professional partners. Their technical guidance, training, and continued engagement supported student research, experimentation, professional development, and preparation for careers in space cybersecurity. These partnerships helped advance CHIRP's mission of developing a skilled workforce capable of addressing emerging cybersecurity challenges affecting space and ground systems.

Acronyms and Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CHIRP	Cyber Halo Innovation Research Program
CMU	Carnegie Mellon University
CSUDH	California State University Dominguez Hills
CSUSB	California State University San Bernardino
DSU	Dynamic Software Updates
ETX	Expected Transmission Count
FT-ATO	Fast Track Authority to Operate
GPS	Global Positioning System
IDS	Intrusion Detection System
MRHOF	Minimum Rank with Hysteresis Objective Function
NASA	National Aeronautics and Space Administration
NOS3	Operational Simulator for Space Systems
PCAP	Packet Files
PIDS	Provenance-Based Intrusion Detection System
PNNL	Pacific Northwest National Laboratory
PQC	Post-Quantum Cryptography
RMF	Risk Management Framework
RPL	Routing Protocol for Low-Power and Lossy Networks
SPARTA	Space Attack Research and Tactic Analysis
SSC	Space Systems Command
TLE	Two-Line Element
TSK	Tasks, Skills, Knowledge
USSF	Unite States Space Force
UTEP	University of Texas El Paso
VM	Virtual Machine
ZT	Zero Trust
ZTARV	Zero Trust Architecture Rapid Validation

Contents

Executive Summary ii
Acknowledgments iii
Acronyms and Abbreviations iv
1.0 Introduction 1
2.0 Student Research Overview 2
3.0 CHIRP Student Research Topics 4
3.1 Cohort 1 California State University San Bernardino (CSUSB) 4
3.1.1 Year One Team Research 4
3.1.2 Fast-Track Authorization to Operate- Abigail Gutierrez Deniz and Aubrie Kendall 4
3.1.3 Space Cyber Test Range- Jason Handen and Darlene Tarin 4
3.2 Year Two Individual Research 4
3.2.1 Space Domain Cyber-Attack Awareness- Abigail Gutierrez Deniz 4
3.2.2 Post-Quantum Cryptography Performance Assessment- Jason Handen 5
3.2.3 AI-Enabled Space Security- Darlene Tarin 5
3.3 Cohort 2 University of Texas El Paso (UTEP) 5
3.3.1 Year One Research Topics 5
3.3.2 Quantum Computing for Satellite Intrusion Detection- Viviana Cadena 5
3.3.3 Data Provenance-Based Intrusion Detection- Jose Raul Chaidez 5
3.3.4 Space-Vehicle Fingerprinting- Nicholas Sanchez 6
3.3.5 Improved Routing for Low-Power and Lossy Networks—Kevin Cadena 6
3.3.6 Self-Healing Satellite Communications- Juan Enriquez 6
3.3.7 Generative AI Applications in Satellite Systems- Isabella Garcia 6
3.4 Year Two—Group Research and Demonstrations 6
3.4.1 Generative AI Risks, Ethics, and Security- Raul Chaidez, Kevin Cadena, Viviana Cadena, and Isabella Garcia 6
3.4.2 Threatify: AI-Enabled Network Anomaly Detection- Kevin Cadena and Isabella Garcia 7
3.5 Cohort 3 7
3.5.1 Year One- Group Research CSUSB, UTEP California State University Dominguez Hills (CSUDH) 7
3.5.2 Resilient Space Systems- Christopher Adeniji, Camilah Anguiano, and Yaritza Chinchilla (CSUDH) 7

3.5.3 Space Jam: Assessing Security Threats and Risks of Satellite-to-Satellite Proximity in Orbit- Claudia Ramirez and Priscila Cruz-Garcia (CSUSB) 7
3.5.4 Satellites vs. Fiber: Evaluating the Viability of a National Communication Shift—Evelyn Mejia, Amias Ainsworth, and Julian Elizondo (CSUSB) 7
3.5.5 AI Anomaly Detection for Space Systems Mia Villela and Diego Acosta (UTEP) 8
3.5.6 Kessler Syndrome: Using AI to Assist in Mitigating Space Debris—John Michael Betancourt and Miguel Padilla (UTEP) 8
3.6 Year Two—Demonstration Proposals 8
3.6.1 Neural-Network-Inspired Satellite Coverage Planning Julian Elizondo and Miguel Padilla (UTEP) 8
3.6.2 Dynamic Software Updates and Self-Healing Systems Camilah Anguiano and Yaritza Chinchilla (CSUDH) 8
3.6.3 Hybrid National Communications Architecture Evelyn Mejia, Amias Ainsworth, and Julian Elizondo (CSUSB) 8
3.6.4 AI Training Dataset for Satellite Intrusion Detection Diego Acosta (UTEP) 8
3.6.5 QKD Synchronization-Drift Simulation Evelyn Mejia (CSUSB) 9
3.6.6 SENTRY: Satellite Proximity Threat Alert Claudia Ramirez and Amias Ainsworth (CSUSB) 9
3.6.7 Explainable AI for Satellite Telemetry Mia Villela and Priscila Cruz-Garcia (UTEP) 9
3.7 Future Research, Development, and Potential Applications 9
3.7.1 Integrated Mission Assurance 9
3.7.2 Adaptive Zero Trust and Resilient Software 9
3.7.3 AI-Enabled Cyber Defense and Data Management 10
3.7.4 Space-Domain Threat Correlation 10
3.7.5 Resilient Communications and Quantum Security 10
3.7.6 Cyber-Range Validation and Human-Machine Teaming 10
4.0 Impact & Accomplishments 12
4.1 Notable Student Accomplishments 12
5.0 Conclusion 14

1.0 Introduction

CHIRP was a research driven program built around students pursuing their degrees in cybersecurity, computer science, and engineering. The student's cybersecurity research was applied in support of the missions of SSC S6, a field command of the United States Space Force (USSF). CHIRP provided a collaborative environment where cybersecurity students could grow into a skilled workforce while producing research that strengthened the national security capabilities of SSC and SSC's space industry partners.

CHIRP was a partnership among Pacific Northwest National Laboratory (PNNL), SSC S6, space industry partners, and academic institutions. Through mentored, space mission relevant research projects, CHIRP students contributed directly to solving SSC aligned cybersecurity challenges while building professional readiness. The program also advanced a core mission of broadening the cybersecurity talent pipeline, and helped create a more innovative, resilient, and representative workforce for SSC and the broader space enterprise.

CHIRP students conducted research aligned to critical workforce and mission needs, including network security, cyber analysis, incident response, cyber policy, data architecture, continuity of operations, data analytics, machine learning, AI, and secure software development. Students focused on SSC mission-specific problems, translated research into practical insights, prototypes, and recommendations that would inform future capability development for SSC and partner organizations. Many students have gone on to graduate and enter roles supporting SSC and participating industry partners, including students continuing into advanced degree programs aligned with the space-cyber mission.

PNNL supported university outreach efforts, student development, and program management, and facilitated engagement with SSC leadership, universities, and space industry partners to ensure that the students' research remained mission-relevant and impactful.

This report summarizes the impact of CHIRP students' research, the outcomes and contributions of their work, and recommendations for future research applications and development across SSC, and the space industry.

2.0 Student Research Overview

By participating in CHIRP, students engaged directly in space-cyber research and were able to investigate relevant cybersecurity applications, test their ideas, build prototypes, and produce defensible findings for space related missions. This student-centered research approach was important in the space-cyber domain, where rapidly evolving threats, complex system dependencies, and high mission assurance demands require professionals who can think critically, validate their solutions, and clearly communicate risk and impact to technical and non-technical stakeholders.

The research topics were selected through a joint, collaborative process between partnering universities, PNNL and SSC, ensuring that students' work was grounded in authentic mission context and connected to real space centric priorities. Topic areas were chosen to provide CHIRP students with strong educational experiences while also supporting SSC's mission goals, near term actions, and longer-term capability development. When PNNL and SSC reached consensus, these topics were introduced to the students as a set of high-impact research directions. The CHIRP team provided a space for student innovation and mentor guidance. Students selected one or more research areas to focus on during their time with CHIRP. If the student requested to pursue their own research topic, the program supported that work if it was feasible and appropriate. On-going support was available to ensure its viability. This approach ensured that the students' research remained mission-aligned, reinforcing the program's belief that students produce their best work when they have both clear relevance and genuine ownership.

Research topics spanned a wide range of cybersecurity and technical domains that were deemed relevant to SSC, including information technology, computer science, network security, cyber analysis, incident response, cyber policy, data architecture, continuity of operations, data analytics, machine learning, AI, and secure software development. This interdisciplinary approach was intentional because SSC's mission environment required professionals who can operate across technical, operational, and policy boundaries. CHIRP student research created a pathway for developing depth in these specialized areas while also learning how their work connects to broader systems, stakeholders, and mission outcomes.

Students operated within a clearly defined scope of work that began with developing a hypothesis and a comprehensive research plan. This initial phase ensured that their research efforts were focused and grounded in relevant mission needs. Once their plan was established, students conducted structured open-source background research to build a solid foundation for their investigations. This step was essential for understanding the context and refining their approach before moving forward. Students then executed necessary testing, analysis, and prototype development as appropriate for their research topic. This allowed them to validate their hypotheses and produce practical solutions tailored to space-cyber challenges. The deliverables also included a final technical research paper documenting the problem statement, methods, results, and recommendations. Students presented a prototype demonstration of their proof-of-concept work. These often included including scripts, analytic workflows, detection logic, reference implementation, models, simulations, or secure coding examples that could be evaluated or adapted for operational use.

The students participated in formal briefings, which included technical check-ins and guidance sessions to share their findings, discuss limitations, and outline proposed next steps. Students developed supporting materials for their research to include executive summaries, slide presentations, architecture diagrams, datasets, testing plans, evaluation results, and prepared formally structured research proposals. These deliverables were provided to SSC leadership

and their technical teams, PNNL mentors and program leadership, and, to relevant industry partners and academic partners supporting the SSC mission.

The research lifecycle was central to why the students were successful. This approach equipped students with the ability to frame problems effectively, question underlying assumptions, choose the most suitable research methods, and construct evidence-based solutions. It emphasized the development of advanced Tasks, Skills, and Knowledge (TSK), which extended well beyond proficiency with standard cybersecurity tools. Students gained practical experience with relevant technologies and methodologies, developed a strong questioning mindset and analytical discipline, and acquired essential technical and professional skills.

To further assist students' success, each student received specialized training and was assigned to a seasoned mentor during and after their time with CHIRP. Mentorship is foundational for producing excellent research outcomes. The mentors helped the students refine their research questions, validate their approaches to their research problems, access the appropriate tools and methods to use, interpret their results, and translate their findings into deliverables that were credible and useful to SSC. Students were required to work with their mentors on novel applications and research in cybersecurity and to present their research after completion, reinforcing the expectation that their work would be not only innovative, but also communicable, defensible, and actionable. Mentors supported students in developing essential soft skills, including understanding workplace expectations, strengthening presentation styles and techniques, and building effective professional relationships with colleagues and peers.

CHIRP set clear objectives that emphasized both skill development and professional growth. Students engaged in certification training to strengthen and validate their technical capabilities, participated in conferences to expand professional networks, gained exposure to emerging advancements, and practiced communicating technical work in professional environments. The students also contributed to community outreach efforts that fostered social responsibility and strengthened the broader cybersecurity talent pipeline. Students participated in space cybersecurity focused competitions and hands-on activities that provided practical training essential for capability development. This helped them connect theory to real-world execution and decision making under certain constraints. These program elements reinforced the research mission by building students who can not only generate insights but also operate effectively as professionals in varied and complex mission and sector settings.

Students who successfully completed CHIRP requirements are committed to two years of civil service, creating a direct pathway for research-trained talent to contribute to the national security workforce. This pathway also included job opportunities with other federal agencies and contracted industry partners, reflecting the program's broader purpose of strengthening the space-cyber ecosystem.

Through mission-aligned topic selection, mentor-supported student research, professional development activities, defined deliverables, and a structured service pathway, CHIRP placed student research at the center of its program. Student research became the main force behind the program's impact. CHIRP produced students who could do more than fill roles. It developed professionals capable of innovation, critical evaluation, and evidence-based decision-making, while generating research products that would inform future capability development for SSC, USSF, and their industry partners. In an environment where both threats and technologies evolve rapidly, CHIRP's research approach strengthened mission assurance and built the workforce capacity needed for future space cybersecurity applications.

3.0 CHIRP Student Research Topics

This section summarizes the research conducted by each CHIRP cohort, including research topics, methodologies, key findings, demonstrations, and potential applications relevant to SSC and its mission partners.

3.1 Cohort 1 California State University San Bernardino (CSUSB)

3.1.1 Year One Team Research

During the first year, Aubrie Kendall, Abigail Gutierrez Deniz, Darlene Tarin, and Jason Handen conducted team-based research on Zero Trust (ZT). Aubrie Kendall was the only master's student to participate in and complete CHIRP.

The team examined the following research question:

How effectively can the Zero Trust Architecture Rapid Validation (ZTARV) methodology accelerate the identification, assessment, and mitigation of cyber risks to mission-critical systems compared with traditional ZT implementation approaches?

The research presented ZTARV as a systematic methodology for rapidly evaluating and improving ZT network designs in contested cyberspace environments. Using a virtualized testbed and digital-twin framework, ZTARV supported vulnerability identification, mission-focused risk assessment, and iterative refinement of security controls. Its five-step process provided a structured method for bridging ZT concepts and operational implementation requirements. The methodology demonstrated potential to strengthen cybersecurity posture, reduce opportunities for lateral movement, and improve decision-making by cybersecurity personnel and military operators.

Following completion of the ZT research, students were assigned SSC mission-relevant topics.

3.1.2 Fast-Track Authorization to Operate- Abigail Gutierrez Deniz and Aubrie Kendall

The research examined the Fast-Track Authorization to Operate (FT-ATO) process to identify practices for streamlining selected Risk Management Framework activities while preserving operationally informed risk decisions. The study identified FT-ATO as a potential lower-cost and more efficient approach for reducing contractor barriers, improving control implementation, and supporting continuous improvement across the space-cyber environment.

3.1.3 Space Cyber Test Range- Jason Handen and Darlene Tarin

As part of ongoing work with SSC on the Space Cyber Test Range, the team built, integrated, and tested CMU Ghosts across a multi-virtual-machine environment. The capability simulated realistic user activity and supported identification of full-network deployment requirements. The effort provided insight into scaling CMU Ghosts as a low-cost, flexible capability for improving cyber-training realism and evaluating system performance.

3.2 Year Two Individual Research

Following completion of the first year, Aubrie Kendall graduated from CSUSB and began working at PNNL in supply chain risk management. The remaining cohort members continued their research into a second year.

3.2.1 Space Domain Cyber-Attack Awareness- Abigail Gutierrez Deniz

The research developed a capability that integrated the National Aeronautics and Space Adminstration (NASA) Operational Simulator for Space Systems (NOS3) with the Space Attack

Research and Tactic Analysis (SPARTA) framework. The integrated environment supported simulation of cyberattack scenarios, vulnerability identification, impact assessment, and evaluation of cybersecurity strategies for space-based systems. Integration with a virtual environment also supported immersive training in cyberattack prevention, detection, and response.

3.2.2 Post-Quantum Cryptography Performance Assessment- Jason Handen

The research evaluated the performance effects of post-quantum cryptography (PQC) algorithms across processor types, with emphasis on low-power devices. Testing demonstrated performance degradation across all processor types as security levels increased, with the most significant effects observed on resource-constrained platforms. The results indicated that PQC implementation may present challenges for systems required to meet NSA security requirements while maintaining operational performance.

3.2.3 AI-Enabled Space Security- Darlene Tarin

The research examined the use of AI, machine learning, behavioral analytics, and automated threat detection to identify cyberattack patterns and support cyber response activities in space systems. The study considered requirements for detecting defined attack types, meeting established performance objectives, and maintaining compatibility with satellite systems, NOS3, and SPARTA. It also assessed how simulated environments could support development, testing, validation, and personnel training without exposing operational systems to risk.

3.3 Cohort 2 University of Texas El Paso (UTEP)

3.3.1 Year One Research Topics

During the first year, Cohort 2 students conducted individual research on topics relevant to space cybersecurity and mission assurance. Each student developed a research question, conducted a literature review, selected appropriate analytical or experimental methods, evaluated relevant data or representative use cases, and documented the results in a research paper and conference poster. Program mentors provided subject-matter expertise, methodological feedback, and support in refining objectives, interpreting results, and assessing mission relevance.

Research topics included quantum-enabled intrusion detection, data provenance, space-vehicle identification, low-power network routing, self-healing communications, and AI applications for satellite systems.

3.3.2 Quantum Computing for Satellite Intrusion Detection- Viviana Cadena

The research theoretically examined the application of quantum-computing principles to intrusion detection for satellite systems. The study assessed whether quantum-enabled approaches could support real-time network-traffic analysis, anomaly identification, and processing of computationally intensive encrypted data. Because of current technology and implementation constraints, the study did not develop or operationally test a quantum-enabled intrusion detection system.

3.3.3 Data Provenance-Based Intrusion Detection- Jose Raul Chaidez

The research evaluated data provenance—the origin, lineage, and processing history of data—as a means of improving intrusion detection and supporting cyberspace defense. The study examined the Provenance-Based Intrusion Detection System known as UNICORN. The

experimental environment used CamFlow for provenance capture, Kali Linux for authorized penetration testing, and UNICORN for analysis.

Results indicated that provenance-based detection may identify advanced persistent threat activity missed by conventional systems but may require additional processing. The study also identified parsing errors within the experimental process.

3.3.4 Space-Vehicle Fingerprinting- Nicholas Sanchez

The research evaluated space-vehicle fingerprinting techniques to support space domain awareness, object identification, and mission assurance. Simulated tracking hardware modeled on the BlackBox system generated unique GPS signatures and vehicle identification numbers. Results indicated that the approach may support more timely and accurate identification of orbital objects than conventional radar tracking.

3.3.5 Improved Routing for Low-Power and Lossy Networks—Kevin Cadena

The research evaluated a scaled Expected Transmission Count (ETX) metric for the Routing Protocol for Low-Power and Lossy Networks (RPL). The approach was integrated with the Minimum Rank with Hysteresis Objective Function (MRHOF) to penalize higher-ETX links and prioritize more reliable paths. Testing demonstrated a marginal improvement in packet-delivery ratio and reduced energy consumption across the evaluated ranges.

3.3.6 Self-Healing Satellite Communications- Juan Enriquez

The research examined self-healing algorithms for improving the cyber resilience and mission assurance of satellite communications. Machine learning methods were assessed for their potential to detect and mitigate cyber threats, particularly anti-jamming scenarios. A satellite simulator introduced controlled disruptions to transmitted data to evaluate approaches for maintaining communications during interference or attack conditions. The study addressed autonomous detection, mitigation, and recovery as methods for improving the integrity and reliability of satellite communications.

3.3.7 Generative AI Applications in Satellite Systems- Isabella Garcia

The research examined the use of AI, machine learning, and deep learning to address performance, cybersecurity, and scalability challenges in satellite communications. A literature review assessed applications including beam hopping, anti-jamming, network-traffic forecasting, and energy management. The study also considered safety, reliability, security, and ethical requirements associated with AI-enabled space operations.

3.4 Year Two—Group Research and Demonstrations

During the second year, students worked collaboratively to develop proof-of-concept demonstrations. Each group defined the demonstration objectives and approach and obtained leadership review and concurrence before proceeding.

3.4.1 Generative AI Risks, Ethics, and Security- Raul Chaidez, Kevin Cadena, Viviana Cadena, and Isabella Garcia

The research examined the responsible and secure use of generative AI in government and mission-focused environments. Findings emphasized the need for human oversight, governance, security controls, bias detection, and bias mitigation.

3.4.2 Threatify: AI-Enabled Network Anomaly Detection- Kevin Cadena and Isabella Garcia

The demonstration developed an AI-enabled network-traffic analysis capability using a model from the Hugging Face Transformers library and datasets representative of common network attacks. A Python-based backend accepted PCAP or CAP files, parsed the traffic, and prepared it for model analysis. A user interface displayed assessment results, confidence levels, and identified areas of concern. The demonstration provided a basis for evaluating AI-supported network analysis in blue-team and purple-team environments.

3.5 Cohort 3

3.5.1 Year One- Group Research CSUSB, UTEP California State University Dominguez Hills (CSUDH)

During the first year, Cohort 3 students worked in groups to conduct research relevant to space systems, cybersecurity, and mission assurance. Consistent with the approach used by the previous cohort, each group developed a research question, conducted a literature review, selected appropriate methods, evaluated representative data or use cases, and documented its findings in a research paper and conference poster. Program mentors provided additional support in refining objectives, applying methodologies, interpreting results, and assessing mission relevance.

Research topics included resilient space systems, satellite proximity threats, hybrid communications, AI-enabled anomaly detection, and space-debris mitigation.

3.5.2 Resilient Space Systems- Christopher Adeniji, Camilah Anguiano, and Yaritza Chinchilla (CSUDH)

The research examined dynamic software updates (DSU) and self-healing mechanisms for space systems. The literature review assessed scalability, integration with legacy systems, standardized implementation protocols, and real-world validation. The study identified limitations in each of these areas and examined the relationship of DSU capabilities to resilience engineering, autonomic computing, and cyber-physical systems.

3.5.3 Space Jam: Assessing Security Threats and Risks of Satellite-to-Satellite Proximity in Orbit- Claudia Ramirez and Priscila Cruz-Garcia (CSUSB)

The research examined cybersecurity risks associated with inter-satellite links and proximity operations. The literature review identified feasible attack scenarios and assessed existing mitigation frameworks. The study also examined limitations associated with international regulatory agreement, sensitivity surrounding military-owned systems, and the proprietary nature of commercial satellite operations.

3.5.4 Satellites vs. Fiber: Evaluating the Viability of a National Communication Shift—Evelyn Mejia, Amias Ainsworth, and Julian Elizondo (CSUSB)

The research assessed whether long-haul communications could transition from terrestrial fiber, including undersea cables, to an all-satellite architecture. The findings did not support complete replacement of terrestrial infrastructure. Instead, they supported hybrid architectures that integrate satellite and terrestrial communications to improve resilience, redundancy, reliability, and security.

3.5.5 AI Anomaly Detection for Space Systems Mia Villela and Diego Acosta (UTEP)

The research examined how AI-enabled cyber-anomaly detection could support cyber operators protecting space systems. The literature reviews identified challenges involving data scarcity, detection accuracy, and false positives. Few-shot learning and multi-algorithm approaches were examined as methods for improving detection performance.

3.5.6 Kessler Syndrome: Using AI to Assist in Mitigating Space Debris—John Michael Betancourt and Miguel Padilla (UTEP)

The research examined Kessler Syndrome and the effects of inter-satellite links and proximity operations on space-system security. The literature review assessed AI, machine learning, autonomous systems, and robotic systems for detecting, tracking, and mitigating space debris. Findings indicated potential improvements in collision prediction, debris mitigation, and active debris removal.

3.6 Year Two—Demonstration Proposals

During the second year, students developed and built proof-of-concept demonstrations based on their research. Each group defined the operational or technical need, proposed an approach, identified anticipated benefits, and addressed competing solutions, limitations, and implementation challenges.

3.6.1 Neural-Network-Inspired Satellite Coverage Planning Julian Elizondo and Miguel Padilla (UTEP)

The demonstration developed a neural-network-inspired algorithm to optimize satellite coverage planning using publicly available Two-Line Element orbital data. The effort included data acquisition, model training, and performance validation to assess whether neural-network-based weighting could outperform traditional satellite-selection methods. The concept provided initial insight into satellite sequencing, mission coordination, and AI-enabled constellation management.

3.6.2 Dynamic Software Updates and Self-Healing Systems Camilah Anguiano and Yaritza Chinchilla (CSUDH)

The demonstration evaluated scalable DSU frameworks for maintaining space-asset availability while minimizing downtime. Initial testing focused on a single CubeSat, with consideration for expansion to a small CubeSat network. Evaluation areas included performance, security, scalability, legacy-system integration, and seamless software updates across modeled satellite systems.

3.6.3 Hybrid National Communications Architecture Evelyn Mejia, Amias Ainsworth, and Julian Elizondo (CSUSB)

The demonstration addressed physical and cyber threats to fiber-optic networks by examining the integration of satellite, terrestrial, aerial, and Internet of Space Things technologies. The proposed architecture sought to improve reliability, coverage, redundancy, and security across critical infrastructure. The effort also considered interoperability, implementation complexity, QKD limitations, and AI-based network management.

3.6.4 AI Training Dataset for Satellite Intrusion Detection Diego Acosta (UTEP)

The demonstration addressed limitations in existing public datasets for AI-enabled satellite-network intrusion detection. Multiple public datasets were integrated and enhanced using

requirements aligned with SSC mission needs, without incorporating sensitive SSC data. The resulting prototype dataset was intended to support AI model training and improve the accessibility of space-cybersecurity data.

3.6.5 QKD Synchronization-Drift Simulation Evelyn Mejia (CSUSB)

The demonstration examined synchronization drift as a vulnerability in QKD-enabled satellite communications. Drift can reduce photon-timing accuracy and increase the quantum bit error rate, affecting secure key exchange. The proposed simulation modeled QKD encryption behavior and evaluated drift-related effects under controlled conditions.

3.6.6 SENTRY: Satellite Proximity Threat Alert Claudia Ramirez and Amias Ainsworth (CSUSB)

The demonstration examined dynamic token rotation as a means of protecting satellites from cyber and proximity-based threats. The concept integrated network monitoring, proximity detection, and adaptive authentication to update access credentials and respond to suspicious activity. The demonstration provided a basis for evaluating whether rotating identity tokens could improve resilience against unauthorized access and environmental disruptions.

3.6.7 Explainable AI for Satellite Telemetry Mia Villela and Priscila Cruz-Garcia (UTEP)

The demonstration evaluated open-source anomaly-detection models and explainable AI techniques using publicly available satellite telemetry data. The approach sought to identify cyberattack-related anomalies and provide insight into the factors influencing model outputs. The effort addressed the limited availability of explainable anomaly-detection research focused on cybersecurity applications in satellite telemetry.

3.7 Future Research, Development, and Potential Applications

Future efforts could build on Cohort 1–3 findings by evaluating cybersecurity, communications, and resilience capabilities within a representative space mission architecture. A novel approach would establish a mission-thread digital engineering and cyber-range environment that integrates ZT controls, realistic user activity, NOS3, SPARTA, satellite telemetry, orbital data, and representative communications links. This environment could support repeatable test and evaluation under nominal, degraded, disrupted, and contested conditions.

3.7.1 Integrated Mission Assurance

Development could focus on a common framework for evaluating space-system resilience across the mission thread rather than assessing individual technologies independently. The framework could correlate cyber events, system anomalies, communications degradation, proximity activity, and mission effects. Measures such as detection time, response time, recovery time, system availability, communications continuity, operator workload, and mission impact could support comparison of cybersecurity architectures and identification of mission-essential dependencies.

3.7.2 Adaptive Zero Trust and Resilient Software

Future efforts could evaluate adaptive ZT controls for spacecraft and ground systems operating with intermittent communications, limited processing capacity, changing mission roles, and proximity operations. Authentication and access decisions could incorporate spacecraft identity, mission role, orbital position, link behavior, telemetry anomalies, and mission conditions. This capability could be assessed alongside dynamic credential rotation, inter-satellite link monitoring, and least-privilege access controls.

Related development could address secure dynamic software updates and self-healing mechanisms for heterogeneous spacecraft and legacy ground systems. Mission-aware update processes could account for spacecraft availability, communications windows, system criticality, threat conditions, and update-failure risks. Testing could evaluate secure staging, cryptographic verification, rollback, recovery, update prioritization, and continued operations during interrupted or compromised updates.

3.7.3 AI-Enabled Cyber Defense and Data Management

A future development effort could establish space-relevant datasets and standardized evaluation methods for AI-enabled cyber-anomaly detection. Public telemetry, network traffic, orbital data, and controlled synthetic events could represent normal operations, equipment faults, environmental effects, communications disruptions, and cyber incidents. Evaluation could compare few-shot learning, multi-algorithm detection, synthetic-data generation, and explainable AI using measures such as detection accuracy, false-positive and false-negative rates, processing requirements, model confidence, explainability, and operator workload.

A novel application would combine data provenance and explainable AI to provide traceable cyber-event analysis. Provenance could reconstruct the sequence of activities associated with a suspected intrusion, while explainable models could identify the factors supporting an alert. These capabilities could support incident reconstruction, threat characterization, operator decision-making, and auditable cyberspace defense activities while preserving human review and decision authority.

3.7.4 Space-Domain Threat Correlation

Future development could integrate satellite telemetry, network activity, orbital position, proximity events, inter-satellite link behavior, and space-debris data to improve threat characterization. The capability could assist in distinguishing friendly, unknown, malfunctioning, or potentially hostile objects and differentiating cyber incidents from equipment faults, environmental effects, and orbital hazards. AI-generated assessments could support event prioritization and course-of-action development, provided that model reliability, data quality, adversarial manipulation, and the consequences of inaccurate assessments are evaluated.

3.7.5 Resilient Communications and Quantum Security

Pilot demonstrations could evaluate hybrid communications architectures that integrate satellite, terrestrial, aerial, and emerging space-based networks. Testing could assess how communications paths are selected and reconfigured when links are degraded, disrupted, or compromised. Measures could include latency, availability, routing efficiency, cybersecurity, interoperability, operational separation, energy consumption, and mission continuity.

A novel extension would incorporate cyber-threat indicators into routing decisions so that path selection accounts for both technical performance and potential compromise. Additional development could assess post-quantum cryptography (PQC) migration strategies for resource-constrained spacecraft and ground systems, including effects on processing, power, memory, latency, and system availability. QKD research could examine synchronization drift, platform motion, atmospheric effects, photon timing, quantum bit error rate, link interruption, and key-exchange recovery.

3.7.6 Cyber-Range Validation and Human-Machine Teaming

The Space Cyber Test Range could be expanded to evaluate these capabilities in combination. CMU Ghosts or similar tools could generate representative user and system activity, while NOS3 and SPARTA could provide space-system and threat contexts. Testing could examine

ZT controls, AI-enabled detection, provenance analysis, PQC performance, adaptive routing, software updates, proximity threats, and recovery procedures.

The primary novel application would be evaluating cross-domain effects—for example, how a cyber anomaly affects routing, how routing changes affect mission availability, or how a software update affects detection and recovery. Human-machine teaming assessments could measure alert quality, explanation utility, operator workload, decision time, training requirements, and trust in automated recommendations.

Collectively, these efforts could provide SSC and its mission partners with a structured path for developing and evaluating integrated capabilities that support mission assurance, cyberspace defense, space domain awareness, communications resilience, and recovery. Additional development, operationally representative testing, cybersecurity assessment, and leadership concurrence would be required before transition to acquisition activities or operational use.

4.0 Impact & Accomplishments

The CHIRP student cohort made significant strides in narrowing key research gaps within space cybersecurity, demonstrating the value of mission-relevant experimentation and interdisciplinary collaboration. By conducting hands-on space cybersecurity experiments and engaging in research that bridged cyber, autonomy, computer science, and policy, they not only advanced technical knowledge but also fostered a culture of innovation. Their efforts opened new avenues for applied research with diverse partners, strengthened the CHIRP program's network, and broadened its impact. Importantly, the students helped develop a robust workforce pipeline, increased awareness of the urgent need for space-cyber specialists and pioneered novel approaches as the field evolved. Their accomplishments underscored the importance of student-led research in driving operational solutions for national defense, while laying the groundwork for future advancements in space-cybersecurity and inspiring the next generation of talent to address emerging challenges in this critical domain.

4.1 Notable Student Accomplishments

Cohort 1 Research Recognition

- Responded to DoD Cybersecurity University Consortium Request for Information: Cohort 1 students from CSUSB, developed research addressing critical cybersecurity topics, including ZT implementation at the tactical warfighting edge and mission-focused cyber-risk management.
- Developed ZTARV: The cohort proposed a structured methodology for rapidly assessing ZT network designs, identifying vulnerabilities, evaluating mission risk, and refining security controls in contested cyberspace environments.
- Received National Recognition: The cohort's research paper was selected for first place in its category among nationwide submissions. The recognition demonstrated the students' ability to develop actionable research aligned with operational cybersecurity and national defense requirements.
- Supported Professional Publication: Following the competition, the students were invited to submit an adapted version of their research for consideration by Joint Force Quarterly, published by National Defense University Press.

Applied Cybersecurity Training

Completed CT Cubed, Inc. Training: Five CHIRP students completed cybersecurity training provided by CT Cubed, Inc., and received certificates of completion. This training addressed cybersecurity tactics, techniques, and technologies relevant to aerospace, critical infrastructure, and other high-risk environments, including:

- Cybersecurity assessments
- Cyber-range implementation
- Mission-focused engineering
- Workforce development
- AI applications in operational environments
- Security, trust, and resilience considerations for mission-critical systems

The training also complemented student research by providing practical exposure to applied cybersecurity, cyber-range operations, AI-enabled cybersecurity, and the protection of mission-critical systems.

Professional Certifications and Credentials

CHIRP students earned certifications and credentials in the following areas:

- Certified in Cybersecurity
- CompTIA Security+
- Certified Ethical Hacker
- AI for Cybersecurity and Bug Bounty Hunting
- Cloud Security and Audit Fundamentals for:
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- Magnet Certified Forensic Examiner
- AccessData Certified Examiner for Forensic Toolkit
- Amateur Radio Technician License
- GIAC Foundational Cybersecurity Technologies (SANS)
- Microsoft Technology Associate: Software Development Fundamentals (MTA)
- Cybersecurity Fundamentals for Space

These credentials expanded student competencies in cybersecurity operations, ethical hacking, cloud security, digital forensics, software development, communications, artificial intelligence, and space cybersecurity.

ISC2 Partnership

The CHIRP program established a partnership with the International Information System Security Certification Consortium (ISC2) to provide students with access to its entry-level Certified in Cybersecurity credential. ISC2 provided participating CHIRP students with training, examination preparation, and examination vouchers at no cost.

The partnership enabled students to obtain a globally recognized entry-level cybersecurity certification before graduation and provided a foundation for pursuing additional certifications and employment in the cybersecurity field. Although the certification was not established as a specific SSC or Space Force requirement, it supported CHIRP's workforce-development objectives by improving student readiness for cybersecurity employment and continued professional development.

5.0 Conclusion

Throughout the program, CHIRP students addressed mission-relevant challenges in space cybersecurity through structured research, interdisciplinary collaboration, and applied experimentation. Across the cohorts, students examined ZT architecture, PQC, AI-enabled anomaly detection, data provenance, satellite identification, resilient communications, dynamic software updates, proximity threats, hybrid communications, space-debris mitigation, and AI applications for space systems.

The program progressed from foundational research and literature reviews to individual and group demonstrations, proof-of-concept development, cyber-range experimentation, and mission-focused analysis. Efforts involving ZTARV, CMU Ghosts, NOS3, SPARTA, AI-enabled network analysis, satellite communications, and space-system resilience demonstrated the students' ability to translate technical concepts into practical evaluation methods and prototype capabilities. These activities generated findings relevant to cybersecurity assessment, mission assurance, cyberspace defense, space domain awareness, system resilience, and technology development.

In addition to producing research papers, conference posters, and demonstrations, CHIRP supported student professional development through applied cybersecurity training, industry and government engagement, technical certifications, and workforce-development partnerships. Students earned credentials in cybersecurity, ethical hacking, cloud security, digital forensics, artificial intelligence, software development, communications, and space cybersecurity. Cohort 1 also received national recognition for its Zero Trust research through a Department of Defense University Consortium for Cybersecurity competition and was invited to submit an adapted version of the work to *Joint Force Quarterly*.

Collectively, the work documented in this report demonstrates the value of student-led research in addressing emerging space-cybersecurity challenges. The findings provide insights that may inform operational planning, policy development, cybersecurity requirements, test and evaluation activities, technology adoption, and future research for SSC, USSF, industry partners, and the broader space community. CHIRP also strengthened the space-cybersecurity workforce pipeline by preparing students to apply research, engineering, analytical, and operational skills to evolving national security challenges.

.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov