UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

CROSS DOMAIN COMMAND & CONTROL LAB

COURSES SUPPORTED

- CyS435 Cyber Operations
- Cyber 256 Basic Cyber Operations
- Cadet Cyber Competition Team
- Military Strategic Studies courses

RESEARCH ALIGNMENT

- Cyber integration into Service- and Nation-level exercises
- Air Battle Management System (ABMS)

DESCRIPTION

The Cross Domain Lab is designed to facilitate an immersive and scalable learning environment in order to provide future Air and Space Force leaders with a unique and lasting experience in the fundamentals of warfare and the employment of cyber effects in a dynamic Joint Landscape. Data from multiple sources will be used for simulation, analysis and comprehensive understanding of integrated operations. As a war room, the lab will serve as the operating location for major exercises and training events. This includes access to the Joint Information Operations Range (JIOR) network to tie cadets and faculty into major national and international exercises such as Red Flag or Cyber Flag as well as Air Force Cyber training and exercises.

Further, the Cross-Domain Lab serves as the immersive learning space that incorporates new and developing technologies to provide realistic examples of military technology that cadets will be interacting with in a very short time on active duty. A host of active and former military instructors on staff will provide years of experience to enhance learning outcomes through past, present, and expected future conflict scenarios. This lab creates context for cadets, faculty, staff, and partners, through experiential-learning, to create meaningful, sustained, and inspirational character and leadership growth. Introduces operational careers in cyber and how cyber effects are best integrated into land, sea, air, and space operations.

ROOM FEATURES

- Cleared for up to secret collateral discussions and networks
- JIOR Node – connection to major exercises (e.g. Red Flag or Cyber Flag)
- Up to 30 stations with unclassified/secret collateral network access running Plexys ASCOT-7 System
- 15’ x 30’ data wall

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

IMMERSIVE ENVIRONMENTS, DATA VISUALIZATION & DECISION SUPPORT LAB

COURSES SUPPORTED

- CS474 – Graphics
- CS/CyS/DS/ECE Capstones
- CS362 - Computer Simulation
- CS364 – Databases
- CS471 - Artificial Intelligence
- Behavioral Science and Leadership courses

RESEARCH ALIGNMENT

- Immersive Environments
- Artificial Intelligence/ Machine Learning
- Deep Learning/Neural Networks

DESCRIPTION

This lab will serve as a hardware showcase for Internet of Things (IoT), virtual reality, augmented reality, human-machine interaction, and big data analysis technologies. The space will support sensing, data analytics, decision-making and information visualization tasks. Experimentation, education, training and research will take place in the lab, with a focus on improving the sensing and decision-making abilities of Air Force and Space Force personnel. Cadets in this space will be able to manipulate big data gathered using AI/ML with augmented reality tools; at the same time, the instructor and other cadets will follow along on screens throughout the classroom.

ROOM FEATURES

- Cleared for up to secret collateral discussions and networks
- Precise indoor location tracking (to support Virtual and Augmented Reality Systems)
- Projection / Multi-screen displays on all walls to support persistent data visualization
- Wired connectivity (and device storage containers) near ceiling for IoT devices

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

CYBER SECURITY, NETWORKING, RADIO FREQUENCY & TELECOMM LAB

COURSES SUPPORTED

- CS110 - Intro to Computer Science
- CyS334 - Cyber Defense
- CS467 - Computer Networks
- ECE215 - Principles of Electronic Cyber Wafare
- ECE315 - AF Electronic & Cyber Systems
- ECE333 - Signal Processing & Linear Sys
- ECE348 - Telecommunications
- ECE447 - Comm Sys CS/ CyS/ECE Capstones

RESEARCH ALIGNMENT

- 5G Technologies
- Counter-UAS

DESCRIPTION

This lab will support the evaluation of cellphone signals, Wi-Fi frequencies, unmanned aircraft systems (UAS) control frequencies and more. The lab will feature a fully configurable cybersecurity testing environment capable of small-scale physical and larger-scale virtual network simulations. Researchers will be able to test and analyze malware hidden in network traffic and conduct and evaluate tests on appropriate ranges of the frequency spectrum. In this environment, cadets will have an electrified, signal-isolated space to conduct testing, jamming, interception and other sensitve frequency operations.

ROOM FEATURES

- Faraday Cage
- Antenna pads w/ conduit back to lab
- ESD work bench
- Testing equipment

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

INDUSTRIAL CONTROLS & PLATFORM SECURITY LAB

COURSES SUPPORTED

- CyS435 – Cyber Operations
- ECE311 - Cyber Power
- ECE 382/383 - Embedded Systems
- CyS438/439 – Cyber Science Capstones
- CS110 - Introduction to Computing & Cyber Ops
- ECE Capstones
- CE Capstones

RESEARCH ALIGNMENT

- Security of Industrial Control Systems
- Lightweight Encryption for the Low Powered IoT Devices

DESCRIPTION

This lab focuses on both the attack and defense of critical infrastructure. According to the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." This lab will feature physical and virtual industrial controls for systems such as the electrical power grid, water treatment plants, airspace control, traffic lighting, or police and emergency response networks. A scale model of a town linked to these industrial controls as well as typical building automation devices provide ideal cyber-physical platforms for evaluating offensive and defensive cyber actions involving the integration of these systems.

ROOM FEATURES

- Scale model of a small city with network-connected, low fidelity industrial control systems
- High fidelity replicas of specific real-world industrial systems, such as an electrical power grid, supervisory control computers, and programmable logic controllers
- Smart building automation and management system including-smart devices (lighting, blinds, appliances, etc)
- Rolling equipment simulators
- Joint Information Operations Range (JIOR) node connectivity

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

CYBER FORENSICS & REVERSE ENGINEERING LAB

COURSES SUPPORTED

- CyS333 - Cyber Warfare
- CyS334 - Cyber Defense
- Cyber Science Capstones

RESEARCH ALIGNMENT

- Evolution of malware families
- Cyber security policy and tools
- Penetration testing of DAF systems & networks

DESCRIPTION

Threat hunting and incident response tactics and procedures have evolved rapidly over the last decade. The full-spectrum of Air Force operations rely on information systems and cannot afford to utilize threat hunting techniques that fail to fully understand the impacts of adversary actions and malware. The courses held in this lab teach advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including Advanced Persistent Threats (APT), n ation-state adversaries, organized crime syndicates, and hacktivists.

Students and researchers will conduct digital forensic analyses of computing devices and perform testing and analysis of software to conduct reverse engineering of potential malware. Using malware analysis tools, students and researchers can analyze the attack lifecycle and glean important forensic details to enhance their threat intelligence to stop the spread of attacks and prevent future attacks. The lab will be equipped with access to the Joint Information Operations Range to allow connection to multiple training ranges as well as malware repositories.

ROOM FEATURES

- Malware analysis network/secure sandbox, reverse engineering software
- Write blockers, high-powered examination computers, forensic software
- Access to National, DoD, & AF Cyber Training Environments/Scenarios
- Access to multiple malware repositories
- High-speed, separated networks
- Student pods with a dedicated screen/monitor at each pod

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

ROBOTICS & AUTONOMOUS SYSTEMS LAB

COURSES SUPPORTED

- CS 472 - Autonomous Systems
- ECE210 - Intro to ECE
- ECE387 - Foundations of Robotics Research
- ECE 487 - Fundamentals of Robotics
- CS/CyS/ECE Capstones

RESEARCH ALIGNMENT

- Robotics
- Human-Machine Interface
- Autonomous Algorithms
- Counter-UAS
- Swarming

DESCRIPTION

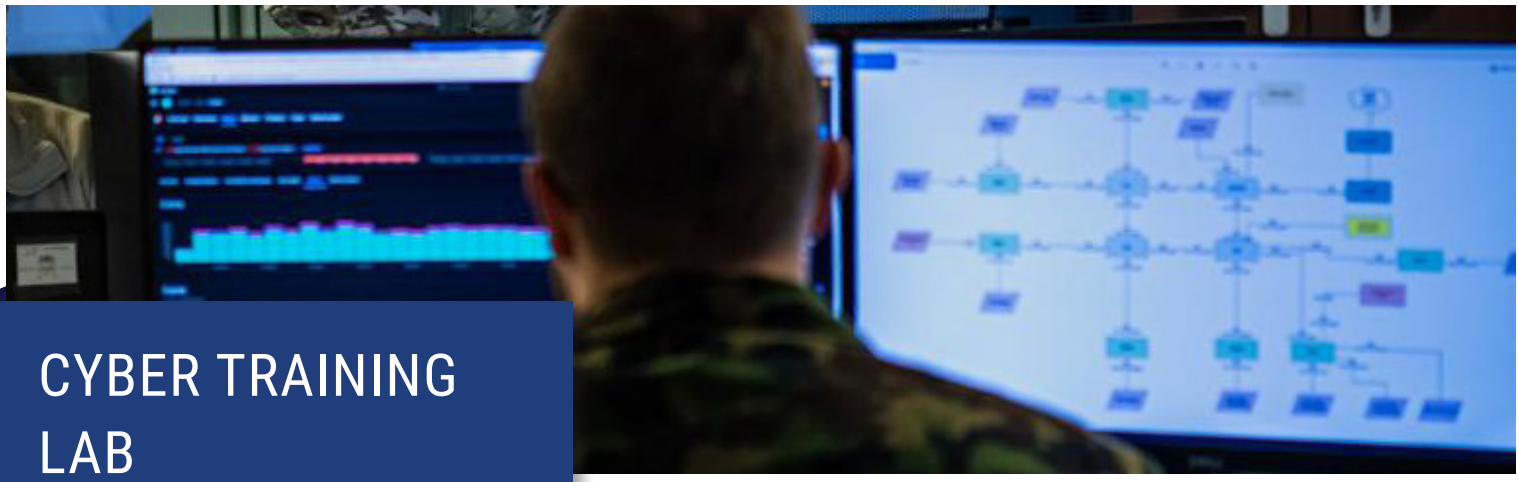
Adversary nations continue to make advances in autonomous weapon systems and swarming Unmanned Aerial System (UAS), i.e., drone, technology. This space allows for research and testing of systems designed to counter these threats. High powered charging stations in this lab allow for the rapid and safe recharging of volatile batteries utilized in UASs and ground-based robotics. A floor to ceiling net allows for the safe indoor flight testing of small quadcopter UASs for class demonstrations and capstone research. Additionally, 3d printers will enable rapid replenishment of UAS parts lost to collisions during testing. Ceiling mounted power and network drops allow installation of simulated GPS, which enables full autonomous navigation functions.

ROOM FEATURES

- Ceiling mounted power & network drops for simulated GPS
- Motion Capture system
- ESD tables
- 3D and circuit printing
- Conduit from lab for antenna connectivity
- Drone swarm programming and analysis
- Ground-based robotics AI/ML testing

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER



CYBER TRAINING LAB

COURSES SUPPORTED

- Cadet Cyber Competition Team
- Summer Cyber Training Prorams

RESEARCH ALIGNMENT

- Cyber operator training effectiveness

DESCRIPTION

This lab will house the Cadet Cyber Competition Team and the Cadet Summer Cyber program. The Cadet Cyber Competition Team competes in national and international cyber competitions. The cyber training lab will provide the platforms and infrastructure necessary to maintain a robust, competitive team year after year. Platform systems are smoothly integrated with operator stations and reconfigurable data walls throughout the room. Cadets from all majors can select the Cadet Summer Cyber program in the summer of their three-degree year. This lab will provide a realistic offensive and defensive space, simulating real-world cyber operations that cadets may experience if they choose the cyber career field. Integration with the ICS lab and Cyber City provides an additional level of realism to these simulations.

ROOM FEATURES

- Re-configurable operator stations
- Movable data walls
- Fiber & copper connections integrated through a raised floor
- Connections to cloud and local infrastructure
- Rapid reconfiguration for summer cyber programs
- Ability to connect to all remote cyber competitions on a low-latency-connection

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

CYBER EDUCATION CLASSROOMS

COURSES SUPPORTED

- CS110 - Introduction to Computing & Cyber Ops

RESEARCH ALIGNMENT

- • Educational strategies in core computer science courses
- USAFA educational outcomes effect on Air Force goals

DESCRIPTION

The state-of-the-art cyber classrooms will service the Computer Science 110 course (CS110) and some advanced computer science and/or cyber science courses. The CS110 course is a mandatory course taken by all cadets their freshman year (~1,200 cadets per year), and it addresses computer programming, cyber operations, and artificial intelligence to educate cadets to solve complex problems using technology. CS110, as well as the advanced courses, leverages experiential learning via hands-on labs, exercises, and projects. These classrooms will use the latest in networking, virtualization, and smart technology to maximize cadet exposure to the high-tech domain and its capabilities and weaknesses.

Due to the ever-changing computing environment and constantly emerging technologies, these classrooms will be highly modular for rapid reconfiguration of workspaces, devices, and networking. This rapid adaptability of the classrooms will be done while maintaining the clean, innovation-focused aesthetics of the classroom.

ROOM FEATURES

- 24 student spaces per classroom
- 4 electrical power outlets & 2 fiber network ports per person
- Individual hideaway student displays to be used as: a second monitor, a mirror of the instructor's display, or a dedicated computer for test environments
- Visible/accessible network infrastructure including routing/switching/security stack displays
- Collaboration tools to support remote learning/VTCs/guest lectures

UNITED STATES AIR FORCE ACADEMY | AIR FORCE CYBERWORX™

MADERA CYBER INNOVATION CENTER

POLICY, STRATEGY, CYBER LAW, ETHICS & DIGITAL HUMANITIES LAB

COURSES SUPPORTED

- Law440 - Cyber Law
- PolSci466 - Cyber Security Policy & Politics
- Eng366 - Digital Humanities, Media, & Communication

RESEARCH ALIGNMENT

- Cyber and the Law of Armed Conflict
- National & International Cyber Policy
- Ethics in the Digital Age
- Data Protection and Privacy Law and Policy

DESCRIPTION

This lab will help cadets explore the many layers of political, strategic, legal and ethical issues inherent to the cyber domain. Researchers will conduct ethnographic research to understand team/decision-maker/OODA loop dynamics. The analysis of these scenarios, and the decisions that are made in response to them, will help shape the course of cyber law and strengthen the application of cyber policies for generations to come. The lab will include equipment for digital photography, 2-D and 3-D scanning, high-motion video, sound and motion capture for collaborative digital humanities research and projects.

The lab's primary function is to support innovative analysis to cutting-edge policy, strategy, legal, and ethical questions related to ongoing and future Department of the Air Force issues. The lab combines the talents of Airmen, Guardians, and industry experts with United States Air Force Academy (USAFA) faculty and cadets to enable foundational and applied experience in humanities and social science research methods, principles, and their real-world application.

The lab also serves as the home for USAFA's Law, Technology, and Warfare Research Cell (LTWRC). Through partnerships with DoD organizations such as United States Space Command (USSC) and Air Combat Command, LTWRC conducts collaborative cutting edge research and outreach in the areas of cyber, space, and emerging technologies. LWTRC is the host for the annual USSC Legal Conference and conducts monthly webinars and presentations on select cyber, space, and technology topics. In addition, the USAFA Cadet Cyber Policy Competition Team will be homed in this space.

ROOM FEATURES

- Equipment for digital photography, 2-D and 3-D scanning, high-motion video, sound and motion capture
- Highly reconfigurable