Air Force Cyberspace Technical Center of Excellence (AF CyTCoE)

AFIT’s AF CyTCoE designation utilizes all four of its schools (School of Engineering and Management, School of Strategic Force Studies, School of Systems and Logistics, and the Civil Engineer School) to execute the education requirements of the Air Force, Department of Defense (DoD) and the federal government in the cyberspace domain.

MISSION: AF CyTCoE’s mission is to enhance the USAF’s ability to develop cyber warriors capable of delivering strategic, operational and tactical effects by leveraging the most cutting-edge technologies and tactics available.

OUTREACH: AF CyTCoE conducts outreach by building relationships with various cyber organizations and communities, supporting AFIT’s ROTC Advanced Cyber Education course, and by developing cyber-related short courses through its Rapid Development Team.

Advanced Cyber Education (ACE) Course: A four-week course for ROTC cadets that consists of an instructional component, cyber war exercises, and cyber officer development days.

Cyber Short Course Development: Short Course Development by AF CyTCoE staff is a tailored approach to creating education and training for the cyber workforce. To address the educational challenges of creating cyber education and training quickly, the development team works with the educational request and needs of government customers. These efforts leverage existing educational material and development of new material to create comprehensive short course solutions to educate and train the cyber workforce on topics that are consistently evolving and changing within the cyber domain.

Graduate Cyber Education Programs

Graduate cyber degrees are conferred by AFIT’s Department of Electrical and Computer Engineering (ENG). AFIT represents a collection of like-minded scholars, students, researchers, and administrators dedicated to the defense programs of the United States. Over eighty percent of students are active duty military officers. These specially-selected officers, in combination with approved civilians and contractors, make the intellectual environment uniquely defense focused. The unique composition of pure civilian faculty, military faculty, and service-retired civilian faculty makes AFIT unlike any other academic institution anywhere.

MASTER’S DEGREES

Master’s degrees are typically 18-month programs starting in August and ending in March.

Master of Computer Science (GCS)
Cyber Security Sequence -
Master of Computer Engineering (GCE)

Master of Science in Cyber Operations (GCO)
Master of Electrical Engineering (GE) - Various Sequences

DOCTORAL DEGREES

Doctoral degrees are typically 36-month programs starting in August and ending in September.

Doctorate of Computer Science (GCS)
Doctorate of Computer Engineering (GCE)
Doctorate of Electrical Engineering (GE)

Course requirements and eligibility for each program can be found on AFIT’s ENG web page at www.afit.edu/ENG

Why AFIT?

AFIT CAPABILITIES:
• Graduate Cyber Ops Education
• Cyber Workforce Development
• Government, Industry & Academic Partnerships
• Classified Research
• Consulting Services
Graduate Research

AFIT Center for Cyberspace Research
The Center for Cyberspace Research (CCR), established in March 2002, conducts cyber security and cyber operations research at the master’s and PhD levels. CCR affiliated faculty teach and direct graduate research focusing on understanding and developing advanced cyber-related theories and technologies, such as critical infrastructure protection, cyber-physical systems, network intrusion detection and avoidance, insider threat mitigation, cyberspace situational awareness, malicious software detection and analysis, software protection, and anti-tamper technologies.

Research Areas

Human Factors in Cyber Weapons
Topics of Study: Autonomy, Artificial Intelligence, Analytics, Insider Threat

Cyber in Multi-domain Operations
Topics of Study: Command & Control, Mission Assurance, Teaching Methodologies

Advanced Networking & Security
Topics of Study: Software Defined Networks, Cloud Computing, Performance, Optimization

Radio Frequency (RF) / Physical Layer
Topics of Study: Wireless, Cellular, RF Intelligence, Electronic Warfare

Reverse Engineering & Cyber Defense
Topics of Study: Malware Analysis, Incident Response & Digital Forensics

Cyber Physical & Embedded Systems
Topics of Study: Industrial Control Systems, Vehicles, Avionics, Internet of Things

Research Labs

Graduate Education in Cyber Operations (GECO) Lab
The Graduate Education in Cyber Operations (GECO) lab is a 48-seat, stand-alone teaching and research classroom. It is used to investigate computer virus growth and eradication, as well as supporting student education and research in cyberspace related activities, to include network defense, network attack, forensics, and software reverse engineering. The GECO lab contains high-performance workstations, each capable of hosting more than 50 virtual machines. Additionally, the GECO lab is connected to CCR’s Virtual Cluster that consists of over 800 GHz of processing power, more than 5 TB of RAM, and more than 130 TB of disk space permitting the hosting of literally hundreds of virtual machines. CCR’s flagship classroom supports cyber related courses such as: Secure Software Design and Development; Advanced Reverse Engineering; Network Operating Systems; Cyber Forensics; Cyber Defense and Exploitation; Mobile, Wireless, and SCADA Device Security; and Cyber Attack.

RF Signal Exploitation Lab (RFSEL)
The RF Signal Exploitation Lab (RFSEL) provides computing and experimental resources supporting sponsored research activity of 10-12 students annually under the supervision of 3-5 faculty members. The lab collectively includes $2M of workstation and collection system hardware for exploiting intentional (communication, navigation, radar, and cyber) and unintentional (components, integrated circuits) RF emissions to characterize and discriminate RF systems. The computing resources are Integrated within the Cyber Defense Network and provide post-collection signal processing capability for 6.1 and 6.2 proof-of-concept demonstrations aimed at enhancing the experimental-to-operational transition of dual-use commercial and military capabilities.

Reverse Engineering Lab (REL)
The reverse engineering lab contains various soldering equipment, a robotic arm for positioning electromagnetic sensors, a surface mount rework station and a 3D printer. We will soon be adding a CNC for machining PCBs.

Cyber-Physical Lab (Cy-Phy Lab)
This lab includes multiple cyber-physical systems for conducting advanced cyber security research. It contains two automotive test beds, an advanced industrial control system testbed, and various mobile units.

• The first automotive testbed consists of a driver interface, multiple emulated vehicle control modules and a simulation engine for conducting simulated driving research.

• The second automotive testbed consists of many electronic control units from an actual car, including the smart key system, engine control module, instrument cluster and infotainment system.

• The industrial control system testbed consists of an Allen-Bradley ControlLogix PLC, HMI and the sensors and actuators needed to represent a water control system.

• The mobile units include hardware-in-the-loop simulations of a wastewater aeration basin, a prison control system, a power substation and various other applications.

Graduate Education in Cyber Operations (GECO) Lab
The Graduate Education in Cyber Operations (GECO) lab is a 48-seat, stand-alone teaching and research classroom. It is used to investigate computer virus growth and eradication, as well as supporting student education and research in cyberspace related activities, to include network defense, network attack, forensics, and software reverse engineering. The GECO lab contains high-performance workstations, each capable of hosting more than 50 virtual machines. Additionally, the GECO lab is connected to CCR’s Virtual Cluster that consists of over 800 GHz of processing power, more than 5 TB of RAM, and more than 130 TB of disk space permitting the hosting of literally hundreds of virtual machines. CCR’s flagship classroom supports cyber related courses such as: Secure Software Design and Development; Advanced Reverse Engineering; Network Operating Systems; Cyber Forensics; Cyber Defense and Exploitation; Mobile, Wireless, and SCADA Device Security; and Cyber Attack.

RF Signal Exploitation Lab (RFSEL)
The RF Signal Exploitation Lab (RFSEL) provides computing and experimental resources supporting sponsored research activity of 10-12 students annually under the supervision of 3-5 faculty members. The lab collectively includes $2M of workstation and collection system hardware for exploiting intentional (communication, navigation, radar, and cyber) and unintentional (components, integrated circuits) RF emissions to characterize and discriminate RF systems. The computing resources are Integrated within the Cyber Defense Network and provide post-collection signal processing capability for 6.1 and 6.2 proof-of-concept demonstrations aimed at enhancing the experimental-to-operational transition of dual-use commercial and military capabilities.

Reverse Engineering Lab (REL)
The reverse engineering lab contains various soldering equipment, a robotic arm for positioning electromagnetic sensors, a surface mount rework station and a 3D printer. We will soon be adding a CNC for machining PCBs.

Cyber-Physical Lab (Cy-Phy Lab)
This lab includes multiple cyber-physical systems for conducting advanced cyber security research. It contains two automotive test beds, an advanced industrial control system testbed, and various mobile units.

• The first automotive testbed consists of a driver interface, multiple emulated vehicle control modules and a simulation engine for conducting simulated driving research.

• The second automotive testbed consists of many electronic control units from an actual car, including the smart key system, engine control module, instrument cluster and infotainment system.

• The industrial control system testbed consists of an Allen-Bradley ControlLogix PLC, HMI and the sensors and actuators needed to represent a water control system.

• The mobile units include hardware-in-the-loop simulations of a wastewater aeration basin, a prison control system, a power substation and various other applications.

Graduate Education in Cyber Operations (GECO) Lab
The Graduate Education in Cyber Operations (GECO) lab is a 48-seat, stand-alone teaching and research classroom. It is used to investigate computer virus growth and eradication, as well as supporting student education and research in cyberspace related activities, to include network defense, network attack, forensics, and software reverse engineering. The GECO lab contains high-performance workstations, each capable of hosting more than 50 virtual machines. Additionally, the GECO lab is connected to CCR’s Virtual Cluster that consists of over 800 GHz of processing power, more than 5 TB of RAM, and more than 130 TB of disk space permitting the hosting of literally hundreds of virtual machines. CCR’s flagship classroom supports cyber related courses such as: Secure Software Design and Development; Advanced Reverse Engineering; Network Operating Systems; Cyber Forensics; Cyber Defense and Exploitation; Mobile, Wireless, and SCADA Device Security; and Cyber Attack.

RF Signal Exploitation Lab (RFSEL)
The RF Signal Exploitation Lab (RFSEL) provides computing and experimental resources supporting sponsored research activity of 10-12 students annually under the supervision of 3-5 faculty members. The lab collectively includes $2M of workstation and collection system hardware for exploiting intentional (communication, navigation, radar, and cyber) and unintentional (components, integrated circuits) RF emissions to characterize and discriminate RF systems. The computing resources are Integrated within the Cyber Defense Network and provide post-collection signal processing capability for 6.1 and 6.2 proof-of-concept demonstrations aimed at enhancing the experimental-to-operational transition of dual-use commercial and military capabilities.

Reverse Engineering Lab (REL)
The reverse engineering lab contains various soldering equipment, a robotic arm for positioning electromagnetic sensors, a surface mount rework station and a 3D printer. We will soon be adding a CNC for machining PCBs.

Cyber-Physical Lab (Cy-Phy Lab)
This lab includes multiple cyber-physical systems for conducting advanced cyber security research. It contains two automotive test beds, an advanced industrial control system testbed, and various mobile units.

• The first automotive testbed consists of a driver interface, multiple emulated vehicle control modules and a simulation engine for conducting simulated driving research.

• The second automotive testbed consists of many electronic control units from an actual car, including the smart key system, engine control module, instrument cluster and infotainment system.

• The industrial control system testbed consists of an Allen-Bradley ControlLogix PLC, HMI and the sensors and actuators needed to represent a water control system.

• The mobile units include hardware-in-the-loop simulations of a wastewater aeration basin, a prison control system, a power substation and various other applications.
Research Labs (cont.)

Human Systems Integration (HSI) Lab
The Human Systems Integration lab permits the measurement of human performance in a controlled environment. The laboratory is equipped with four reconfigurable work stations, permitting individuals or teams of individuals to work as co-located or simulated remote working conditions. Equipped with both NIPRNet and commercial internet with workstations dedicated to either network and administrative control of the workstations on the commercial internet, a variety of experimental protocols can be easily adopted. The laboratory is equipped with physiology monitoring equipment to include EEG, EOG, ECG, and EGG. Recent experiments within the laboratory have spanned from visual detection experiments under custom lighting configuration to various human-machine teaming experiments.

AR/VR Lab
The AR/VR Workspace is dedicated to development of virtual and augmented reality systems for the Center for Cyberspace Research and the Autonomy and Navigation Center (ANT). The workspace is outfitted with both the Oculus Rift and HTC Vive setups connected to workstations powered by the latest COTS graphics cards. Research supported by this workspace includes serious games for cyber education and training, and autonomy and navigation.

CCR & AF CyTCoE Partnerships
The National Air and Space Intelligence Center (NASIC) at Wright-Patterson Air Force Base
The Air Force Research Laboratory (AFRL) at Wright-Patterson Air Force Base
The U.S. Department of Homeland Security (DHS)
The Air Force Life Cycle Management Center (LCMC)
The 24th Air Force (Air Forces Cyber) at Joint Base San Antonio-Lackland, Texas
SAF/CI/CIO A6: The Chief, Information Dominance and Chief Information Officer
The Space & Missile Systems Center at Los Angeles Air Force Base
Air Force Cyber College
Cyber Resiliency Office for Weapons Systems (CROWS)
Air Force CyberWorx
National Institute of Standards and Technology (NIST)
Defense Innovation Unit

Cyber Professional Continuing Education Opportunities at AFIT
In addition to graduate education, AFIT offers several cyber professional continuing education courses through the School of Strategic Force Studies (EX), the School of Systems & Logistics (LS) and the Civil Engineer School (CE). Learn more at www.afit.edu or contact Matthew Dever, Assistant to the Director, Cyber Program Coordination and Outreach, at matthew.dever@afit.edu or 937.255.3636 x4491 for more information.

Cyberspace PCE Courses Directory
School of Strategic Force Studies (EX) - Learn more at www.afit.edu/ex
Cyberspace 200: Joint Intermediate Cyber Operations/Planners
Cyberspace 220: International Cyberspace Education
Cyberspace 300: Joint Advanced Cyber Planners
Cyberspace 350: Executive Development Graduate Experience/C-EDGE

School of Systems & Logistics (LS) - Learn more at www.afit.edu/ls
CYBER 150: Intro to Protection of Mission Critical Function to Achieve TSN
SYS 240: Avionics Cyber Vulnerability Assessment, Mitigation, and Protection
Cyber Test & Evaluation Workshop

Civil Engineer School (CE) - Learn more at www.afit.edu/ce
WTSS 580: Managing Security of Control Systems
Air Force Cyberspace Technical Center of Excellence

*Developing Cyber Warriors Through Education and Research*

[AFIT logo]

[Website link: www.afit.edu/cyber]

Air Force Institute of Technology (AFIT)  I  2950 Hobson Way, Wright-Patterson AFB, OH 45433