Civilian Cyber Fundamentals Course (CCFC) and Cyber Operations Fundamentals Course (COFC)

Phase 0: Course introduction

Phase 1: Policy, Doctrine, and Guidance
- Cyber Policy
- Air Force Doctrine
- Tactics, Techniques, and Procedures (TTP) Fundamentals

Phase 2: Department of Defense and Joint Cyber Organizations
- Command and Control (C2) Relationships
- DoD and Joint Cyber Organizations

Phase 3: Air Force Information and Cyber Operations
- Network Operations Defense Organizations
- Cyberspace Operations (CO) Organizations
- Civilian Resource Organization
- Information-Related Capabilities
- Information Operations (IO) Concepts
- IO Planning

Phase 4, Part 1: Cyber Network Fundamentals
- Introduction to Networking
- Network Security Fundamentals
- Functional Networks
- Transmission Mediums
- Protocols and Ports
- Air Force Network Architecture
- Joint Cyber Operations (JCOR) Simulation Servers

Phase 4, Part 2: Cyber Network Fundamentals
- Basic Telephony Architecture
- Voice over Internet (VoIP) Architecture
- Introduction to Wireless Technologies
- Radio Frequency Identification (RFID) and Radio over Internet Protocol (RoIP)

Phase 4, Part 3: Cyber Network Fundamentals
- Satellite Operations Networks and Architecture
- Industrial Control System (ICS) Introduction and Architecture
- Introduction to Airborne Networks
- Introduction to Battlefield Networks Architecture
- Combat Information Transport System (CITS)

Phase 5: Cyber Law and Ethics

- Cyber Laws
- Cyber Operations Legal Boundaries
- Ethics in Cyber Operations

Phase 6: Cyberspace Operational Concepts

- Network Warfare Operation Capabilities
- Hacking Methodologies
- Exploiting Search Engines
- Social Engineering Methods

Phase 7, Part 1: Cyber Network Threats

- Computer Network Operations (CNO) Threats
- Exploitation and attack of PSTN and VoIP Networks
- Exploitation and attack of Wireless Technologies

Phase 7, Part 2: Cyber Network Threats

- Exploitation and attack of RFID and RoIP
- Exploitation and attack of Satellite Systems
- Exploitation and attack of Industrial Control Systems
- Exploitation and attack of Battlefield Networks

Phase 8: Cyberspace Operations (CO) Planning

- Target Audience Analysis/ Behavioral Influences Analysis
- Mission Planning

Phase 9, Part 1: Cyberspace Operations (CO) Defense and Mitigation

- Cyber Operations Security (CyOPSEC)
- Protocol Abuse and Tunneling
- Computer Network Defense (CND) Response Actions (RA)
- Defending Public Switch Telephone and VoIP Networks
- Mitigating Wireless Technology Vulnerabilities

Phase 9, Part 2: Cyberspace Operations (CO) Defense and Mitigation

- Defending Satellite Systems and Communication Networks
- Integrated Air Defense Systems (IADS) Components
- Defending Battlefield Networks and Tactical Data Links
- Industrial Control Systems (ICS) Defense
- Cyber Incident Handling and Forensics

Phase 10: Virtual Capstone