U.S. ARMY

Cyber Warfare Specialist Training Map

Enlisted (17C) Initial Military Training

Cyber Basic Technical Core (CBTC)

- Programming Fundamentals
- Computer Organization and Architecture
- Operating Systems
- Networking Concepts & Protocols
- Windows
- Linux
- Programming Languages
- Networking IOS
- Protocol & Traffic Analysis
- Wireless Technologies
- Forensics & Incident Response
- Active Exploitation

Cyber Common Technical Core (CCTC)

<u>Operating Systems</u>
Shells and Scripting
Permissions
Processes
Networking and I/O
Auditing and Logging
Key Windows features
- Registry
- Active Directory

Visualization and Containerization
<u>Networking</u>
Packet Analysis
Services and Network Discovery
Industrial Control Systems/SCADA
Filtering Devices
File Transfer, Redirection, and Tunneling
Secure Shell (SSH)
<u>Security</u>
Concepts
- Reconnaissance
- Web Exploitation
- Exploit Development
- Reverse Engineering
- Privilege Escalation/Persistence
- Forensics / Anti – Forensics

Information Environment 101 (IE-101)

Multi-Domain Operations (MDO) Concept
Information Operations
Electronic Warfare
- Cyberspace Domain & Organization Overview
- Joint Cyberspace Overview
- Domain & Organization Overview
- Army DODIN Operations and Defensive Cyberspace Operations
- Offensive Cyberspace Operations

OCO Analyst Core

(NCS Courses; Access & Adjunct Faculty status needed)

CBTs:
- OVSC1100 – Overview of SIGINT Authorities
- OVSC1208 – FISA Amendment Act Section 702
- OVSC1800 – USSID SP0018 Intel Oversight for Analytic Personnel
- CYEC1200 – Basic Adversary Tactics
- CYEC1250 – Basic Cyber Adversary Awareness
- CYEC2150 – CNO at NSA
- NETA1021 – Internet Technologies
- NETA2002 – Orientation to Applied Digital Network Analysis
- NETA2005 – Intro to GSM and GPRS
- RPTG1012 – Basics of SIGINT Dissemination

Classroom-Based:
- CRSK1000 – Intro to SIGINT Development
- CYEC2200 – Advanced Adversary Tactics
- NETA1030 – DNI Gateway Bootcamp
- NETW1002 – Global Comms Capabilities

Cyberspace Response Assessment (CsRA)

(Army developed scenario-based culminating event)

- DCO: 82d Airborne Division is supporting combat operations in and around the Atropian/Donovian
- CSD: 1337 CSD is tasked to emulate/recreate Donovian targets of interest (bridge transport, IR UAS, RF UAS, air radar and anti-aircraft) and develop allied capabilities to go against each while implementing risk reduction measure.
- CMT: 1337 CMT is tasked to leverage intelligence and gain a foothold within Donovian cyberspace to enact DCO-RA and OCO actions to enact D3M activities against targets of interest.

Course Length = 36 Weeks (Ph.1 19 weeks; Ph.2 17 weeks)

U.S. ARMY

Electronic Warfare Specialist Training Map

Enlisted (17E) Initial Military Training

Cyber Electromagnetic Activities Doctrine

- Intro to Electromagnetic Spectrum (EMS)
- Army CEMA Doctrine
- Legal Authorities
- Spectrum Management Operations (SMO)
- Intelligence Disciplines

Electronic Warfare Fundamentals 1

- Math for SIGINT & Digital Signals Processing
- Intro to Physics
- Theory & Principles of Electricity
- Basic Electronics & Electronic Circuits
- Fundamentals of Radio Frequency Communications
- Antenna Theory
- Intro to Wi Fi Technology

Electronic Warfare Fundamentals 2

- Intro to Radar
- Intro to GPS
- Electro Optics
- Software Defined Radios
- Python Programming
- Electronic Attack, Electronic Protect, & EW Support

Operate & Maintain Assigned EW Systems

- Operate EW Test Equipment
- Operate & Maintain CREW Systems
- Operate & Maintain EW Support Systems
- Operate & Maintain Special Purpose EA (SPEA) Systems
- Operate & Maintain EW Modeling & Simulation Systems
- EW Tactical Vehicle Tactics

Capstone

- Electronic Attack, Protect, & EW Support
- Fieldcraft
- Operate & Maintain EW Systems in Field Env.
- Establish Commo
- Maneuver

Course Length = 28 Weeks, 3 Days

Cyber Capability Developer (170D) WOBC

U.S. ARMY

170D WOBC = 72 weeks (18 months)

MODULE A Common Core
- Role and use of Military History for Leaders in the Profession of Arms
- Identity, Climate, and Culture
- Introduction to Inclusion
- MDMP
- CRM for Operational Leaders and Planners

MODULE B Military Writing and Briefing
- Military Writing, PPT, AR 25-50,

MODULE C Problem Solving for Developers
- Thinking Logically
- Assessment

MODULE D Course Integration
- Development Process
- Configure Software Systems
- Testing Process
- Write Test Cases
- Version Control Use
- Operate a Version Control System
- Version Control Architecture and Advanced Use
- Evaluate Repositories and Objects in Git
- Assessment

MODULE E Discrete Math
- Propositional Logic
- Evaluate Logical Propositions
- Numbers and Algebra
- Evaluate Numbers using Algebra
- Sets
- Evaluate Sets using their Operations
- Sequences and Recursion
- Evaluate Sequences using Recursion
- Assessment

MODULE F Python Programming I
- Python Programming I Block 1
- Python Programming I Block 2
- Knowledge and Practical Assessments

MODULE G Python Programming II
- Python Programming II Block 1
- Python Programming II Block 2
- Knowledge and Practical Assessments

MODULE H Project I
- Culminating Event

MODULE I C Programming I
- C Programming I Block 1
- C Programming I Block 2
- Knowledge and Practical Assessments

MODULE J C Programming II
- C Programming II Block 1
- C Programming II Block 2
- Knowledge and Practical Assessments

MODULE K Project II
- Culminating Event

MODULE L Data Structures & Algorithms (DSA) I
- DSA I Block 1
- DSA I Block 2
- Knowledge and Practical Assessments

MODULE M DSA II
- DSA II Block 1
- DSA II Block 2
- Knowledge and Practical Assessments

MODULE N Project III
- Culminating Event

MODULE O Object-Oriented Python (OOP)
- OOP Block 1
- OOP Block 2
- Knowledge and Practical Assessments

MODULE P Project IV
- Culminating Event

MODULE Q Operating Systems (OS)
- OS Block 1
- OS Block 2
- Knowledge and Practical Assessments

MODULE R X86 Assembly Programming
- x86 Block 1
- x86 Block 2
- Knowledge and Practical Assessments

MODULE S Project V
- Culminating Event

MODULE T Networking
- Networking Block 1
- Networking Block 2
- Knowledge and Practical Assessments

MODULE U C Network Programming
- C Network Programming Block 1
- C Network Programming Block 2
- Knowledge and Practical Assessments

MODULE V Python Network Programming
- Python Network Programming Block 1
- Python Network Programming Block 2
- Knowledge and Practical Assessments

MODULE W Event
- Developer Qualification Event

MODULE X Introduction to Cryptography
- Introduction to Cryptography Block 1
- Introduction to Cryptography Block 2
- Knowledge and Practical Assessments

MODULE Y Organizational Processes
- U.S. Cyberspace Operations
- Cyber Mission Force (CMF)
- Supporting Agencies
- Authorities, Policy, and Compliance
- Mission Support
- Requirements Processes
- Operations Processes

Cyber Operations Officer Course (CyOOC)

U.S. ARMY

MODULE B
Operations in the Information Environment & Cyberspace Planning

- Information Environment Foundations
  - Multi-Domain Operations
  - Joint Inter Agency (IA)
  - Information Environment & Operations
  - Electromagnetic Spectrum
  - Electronic Warfare
  - Space Overview
  - DODIN & DODIN Operations
  - Cyberspace Operations Overview
  - Cyber Mission Force Overview
  - NSA / SIGINT System Overview
  - Cyberspace Law and Authorities
  - Cyber Support to Combatant Commands
- Joint Planning Framework
  - Joint Planning Process
    - Overview
    - Step 1: Planning Initiation
    - Step 2: Mission Analysis
    - Step 3: COA Development
    - Steps 4 & 5: COA Analysis & Comparison
    - Step 6: COA Approval
    - Step 7: Plan or Order Development
- Cyberspace Operations Support & Methodologies
  - Cyber Effects and the Joint Targeting Cycle
  - Intelligence Support to Targeting
  - Defensive Cyberspace Methodologies
  - Offensive Cyberspace Methodologies
  - Cyberspace Infrastructure, Access, & Capabilities
  - Commander's Objectives, Targeting Guidance, & Intent
  - Target Development and Prioritization of Effects
  - Target Systems Analysis
  - Organizational Support to Targeting in Cyberspace
  - Target List Management
  - Cyberspace Tools and Capabilities Analysis
  - Commander's Decision and Force Assignment
  - Mission Planning and Force Execution
  - Combat Assessment

MODULE C
Cisco Certified Network Agent

- Semester 1: Introduction to Networks
  - Networking Today
  - Basic Switch and End Device Configuration
  - Protocols and Models
  - Number Systems
  - IPv4 Addressing
  - IPv6 Addressing
  - ICMP
  - Physical Layer
  - Data Link Layer
  - Physical Layer
  - Data Link Layer
  - Address Resolution
  - Basic Router Configuration
  - Network Security Fundamentals
  - Build a Small Network
- Semester 2: Switching, Routing, & Wireless Essentials
  - Basic Device Configuration
  - Switching Concepts
  - STP Concepts
  - EtherChannel
  - FHRP Concepts
  - LAN Security Concepts
  - WLAN Concepts
  - WLAN Configuration
- Enterprise Networking, Security, and Automation
  - Single-Area OSPFv2 Concepts
  - Single-Area OSPFv2 Configuration
  - ACL Concepts
  - ACLs for IPv4 Configuration
  - NAT for IPv4
  - WAN Concepts
  - Network Design
  - Network Troubleshooting
  - Network Virtualization
  - Network Automation

MODULE D
Programming & Scripting

- Describe Python
- Employ Python Language Features
  - Variables, IO,
  - Flow Control
  - Flow Control 2
  - File IO
  - Python Standard Library
  - Data Structures
  - Binary Data
  - Object Oriented Programming
  - Error Handling (Exceptions)
  - Networking
- Final Project
- Develop Python Solutions (Final Exam Practice)
- Develop Python Solutions (Final Exam)

MODULE E
Cyber Common Technical Core (CCTC)

- CCTC-OS
  - Introduction
  - Build Versions
  - PowerShell (PoSh)
  - PoSh Profiles
  - PoSh Remoting
  - Registry
  - Act Dir Serv (ADS)
  - Win Boot Process
  - Linux Boot Process
  - Win Process Validity
  - User Acct Ctrl (UAC) Bypass
  - Linux Process Validity
  - Windows/Linux Artifacts, Auditing, & Logs
  - Virtualization & Containerization
  - Memory Analysis
  - Active Directory
  - Annex Review/Exam
- CCTC-NET
  - Introduction
  - Net Fundamentals
  - Net Reconnaissance
  - Socket Creation & Packet Manipulation
  - Mvmt & Data Transfer
  - Network Filtering
  - Capstone PE
  - Annex Review/Exam
- CCTC-SEC
  - Intro to Pen Testing
  - Web Exploitation
  - Reverse Engineering
  - Exploit Development
  - Post Exploit Review
  - Win/Lin Privilege Escalation & Persistence
  - Multi-Domain Skirmish
  - Annex Review/Exam
  - King of the Hill PE

MODULE F
Electronic Warfare Foundations

- History of EW
- Intro to EMS
- CEMA Doctrine
- EW Authorities & Policies
- Math for EW
- Radio Wave Fundamentals
- Radio Wave Propagation
- Fundamentals of Radio Communication
- Intro to Antenna Theory
- DF Fundamentals
- Intro to SDRs
- EW Range
- Current EW Threats
- Space / NAVWAR / GPS

MODULE G
Mission Commander

- Cyber Mission Authorities
- Collection Requirements
- Mission Profiles
- CMF Capabilities
- JPP
- Targeting
- Mission Planning
- Operation Procedures
- Operational Tools
- Tactical Planning

MODULE G
Cyberspace Response Assessment/Multi-Domain Operations (Capstone)

- Defensive Cyber Ops
  - SDCO Scenario
  - DCO Out-brief
  - Scenario Introduction
- Capabilities Support Development
  - Expeditionary Capabilities Support Operations Scenario
- FTX
  - Operations Order Decomposition & Pre-Combat Checks
  - Operational Preparation of the Environment
  - Cyberspace Warfare in Multi-Domain Operations
  - Recovery
- Offensive Cyber Ops
  - OCO Scenario
  - OCO Out-brief
- Module Summary
- After Action Review

Course Length = 27 Weeks

As of: 4/11/2023 2:36:27 PM

17B CEWO Course

U.S. ARMY

17B CEWO QC = 13.2 weeks (3 months, 1 week)

MODULE A
Introduction
- Course Orientation
- Army EW Vision
- Duties & Responsibilities
- Security briefing
- Pre-test

MODULE B
Electronics
- Theory
- Math for CEWOs
- Theory and principles of electricity
- Intro to the EMS
- Radio Wave fundamentals
- Radio Wave propagation
- Exam

MODULE C
CommsSystems
- Army, Joint, Allied commssystems
- Cellular communications
- Exam

MODULE E
Electromagnetic Attack
- EA Doctrine
- Current and Future EW threats
- US Army EW strategy
- EA methods and techniques
- Conducting EA in the US and Canada
- EW Reprogramming
- EW Ground Systems
- USMC EA systems
- AEA platforms
- Compare and contrast doctrine
- EW Threat research
- Exam

MODULE D
EMS Based Systems
- Fundamentals of Radar
- Characteristics of Electro-Optics
- GPS & PNT
- C-UAS Systems
- Exam

MODULE F
Electromagnetic Support
- ES Authorities
- National SIGINT request process
- De-conflict ES & SIGINT
- ES Systems
- ISR Platforms and Support
- Exam

MODULE G
Electromagnetic Protection
- Spectrum Management Doctrine
- EM Hardening & Shielding
- EMCON
- Emission de-confliction
- Friendly C2 systems and sensor vulnerabilities
- Degrade Operations
- Deception TTPs
- S2AS EME Survey
- Exam

MODULE H
CEMA Support to Operations
- Operational Framework
- Elements of OPART principles of war
- CEMA Support to Maneuver
- CEMA support to tactical tasks
- Army IO doctrine
- Space-based support to CEMA
- Exam

MODULE I
Plan CEMA Support to Operations
- EW Cell
- Intelligence disciplines
- Databases
- IPB
- CEMA focused MDMP
- Integrating EW into targeting
- Theater Air Ground System
- Joint ATO cycle
- Joint request forms
- EW modeling and simulation
- Develop EW TTPs
- Exam

MODULE J
EW Ground Operations
- Prepare for Ground EW ops
- CEMA specific PCC/PCI
- Link Up procedures
- Battlefield survival and Field Craft
- Develop Unit EW Training Programs
- Manage EW Training Programs
- Exam

17D Cyber Capabilities Development Officer BOLC

U.S. ARMY

MODULE A
Common Core & Junior Leader Development

BOLC-B Initial Military Training (IMT) Common Core (CC) for all branches

Required training of all Programmed Tasks from the approved Common Core Task List

Junior Leader Development provides enhanced development of critical skills needed by the 17A.

- Problem Solving
- Critical Thinking
- Military Decision Making Process (MDMP)
- Intelligence Preparation of the Battlefield (IPB)

MODULE B
Development Introduction

- Development Introduction
- Development Best Practices
- Exam

MODULE C
Operations in the Environment

- Introduction to Cyber Mission Force and Larger Information Environments
- Survey of Information-related Capabilities

MODULE D
Basic Development

- Python Fundamentals
- Advanced Python
- Object Oriented Python
- Networking Theory
- Python Networking
- Introduction to C Programming
- Intermediate C, Part 1
- Intermediate C, Part 2
- Data Structures
- C Algorithms
- C Networking
- Operating Systems with C
- Cryptography Fundamentals
- Basic Skill Level Exam

MODULE E
Advanced Development

- Introduction to Assembly
- Reverse Engineering
- Embedded Architectures
- Introduction to Exploitation
- Intermediate Exploitation
- Heap-based Exploitation
- Hardware Hacking
- RF Introduction
- Exploitation Practical

MODULE F
Development Capstone

- Agile Methodologies
- Capstone Project

Course Length = 47 weeks