



United States Army Cyber Center of Excellence

U.S. Army Cyber Corps Cyber Branch Overview

Office of the Chief of Cyber



Chief of Cyber Introduction



Branch Overview Brief



Q&A with Cyber Team

ADMIN NOTES

- Please hold all questions until the Q&A portion.
- Ensure that your mic is muted unless you are actively speaking.
- To ask questions, use the “Raise Hand” function and wait to be called upon, or type your question in the chat window and wait for a response (time permitting).
- When asking a question during the Q&A session, identify yourself as “Cadet” and your last name.



UNCLASSIFIED

Cyber Corps Facts



History

(in brief)

- **Newest Branch in the Army**
- **Cyber Branch Established – 1 Sep 2014**
- **Direct Commissioning Authorized – 27 Oct 2018**
- **Electronic Warfare Integrated into the Branch – 1 Oct 2018**

Size of the Force

(in total authorizations)

Active Component

Officers: **778**

Warrant Officers: **374**

Enlisted Soldiers: **1,805**

Army National Guard

Officers: **216**

Warrant Officers: **189**

Enlisted Soldiers: **873**

Army Reserve

Officers: **123**

Warrant Officers: **114**

Enlisted Soldiers: **258**

Total Force: 4,730



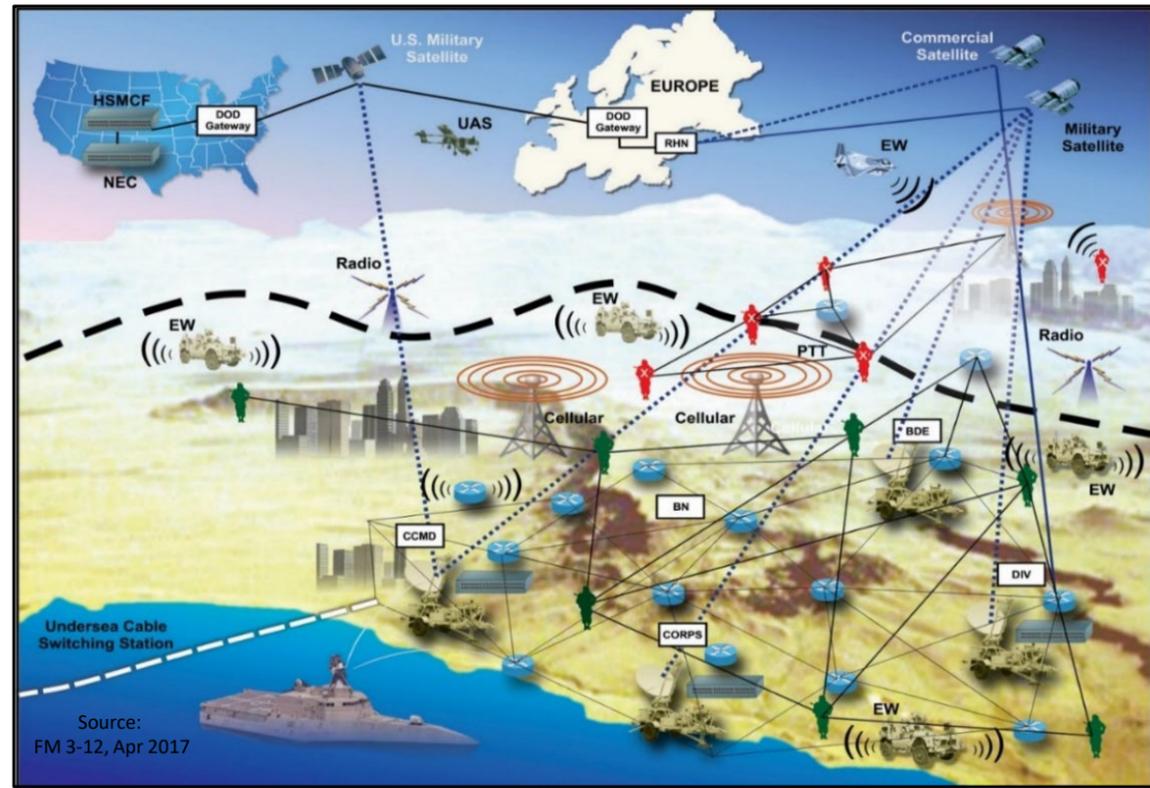
Cyberspace Domain & EMS

UNCLASSIFIED

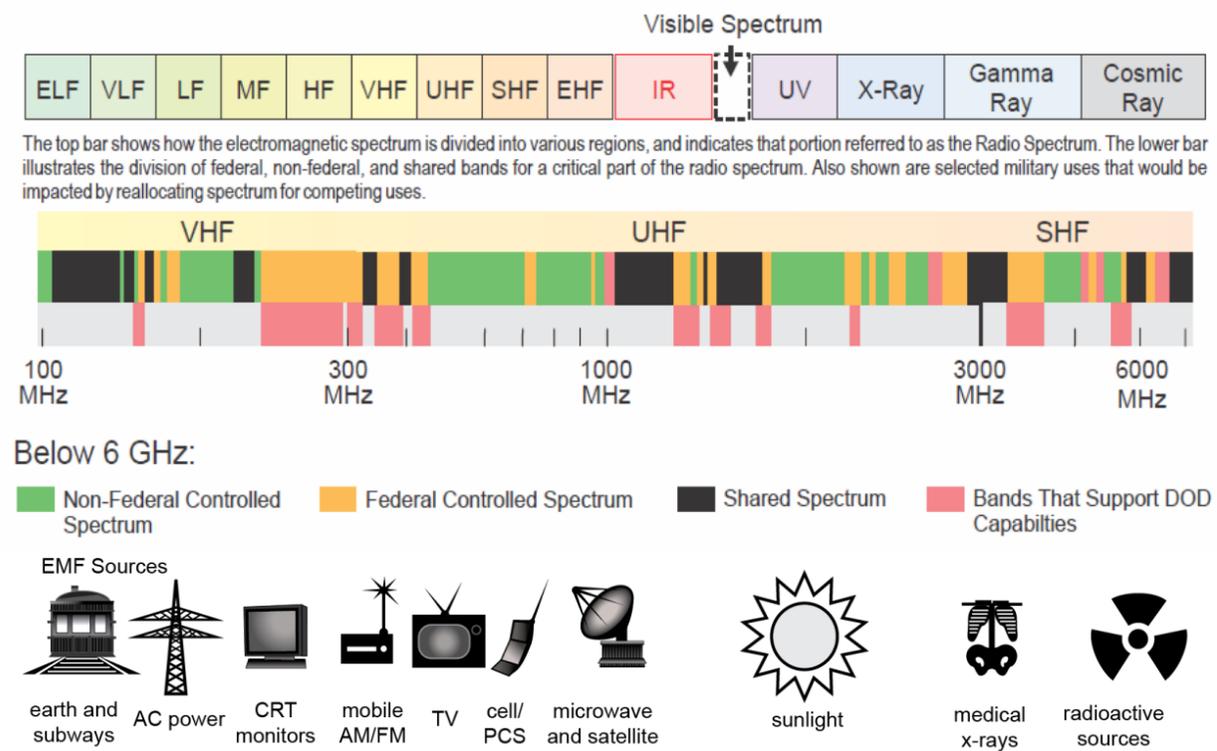


Cyberspace is a global domain within the information environment consisting of the **interdependent network of information technology infrastructures and resident data**, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

The Army performs cyberspace operations and supporting activities within this domain as part of Army and JIM operations.



The Electromagnetic Spectrum



The **Electromagnetic Spectrum (EMS)** is the range of frequencies of electromagnetic radiation from zero to infinity, divided into 26 alphabetically designated bands.

A wide range of equipment operates in the EMS, and many devices that utilize the EMS also utilize cyberspace.

Cyber Corps Careers



17A Cyber Warfare Officer

Cyber Warfare Officers lead, direct, manage, plan, integrate, synchronize, and/or execute Defensive Cyberspace Operations, Offensive Cyberspace Operations, and DODIN Operations at all Army and JIM echelons.

17B Cyber & EW Officer

Cyber & Electronic Warfare Officer lead, direct, manage, plan, integrate, synchronize, and/or execute Cyberspace and Electronic Warfare Operations at Brigade, Division, Corps, Army, and JIM levels.

17D Cyber Capabilities Development Officer*

Leads, directs, manages, plans, integrates, synchronizes, and executes capability development for Cyberspace and Electronic Warfare Operations at Brigade, Division, Corps, Army, and JIM levels.



170A Cyber Warfare Technician

Cyber Warfare Technicians plan, supervise, assess and execute Offensive and Defensive Cyberspace Operations. They provide technical guidance, expertise and advice to commanders and staff on the management and application of Cyberspace Operations.

170B Cyber & EW Technician

Electronic Warfare Technician plans, directs, supervises, assesses, and executes Electronic Warfare operations. They integrate and facilitate Cyberspace Operations at the tactical edge, as required.

170D Cyber Capabilities Developer Technician*

Leads, directs, manages, plans, integrates, coordinates, and develops cyberspace and electronic warfare capabilities for the purposes of executing Cyberspace and Electronic Warfare Operations at Brigade, Division, Corps, Army, and JIM levels.



17C Cyber Warfare Specialist

Cyber Operations Specialists execute Offensive and Defensive Cyberspace Operations in support of the full range of military operations by enabling actions and generating effects across all domains.

17E Electronic Warfare Specialist

Electronic Warfare Specialists are subject matter experts on the manipulation, control, and dominance of the electromagnetic spectrum. They advise and assist the commander or command Electronic Warfare Officer (EWO), as applicable, to defeat the enemy through planning, coordination, integration, and execution of all EW functions.

*Denotes: **Pending Final Army Approval**





Cyber Talent Priorities

UNCLASSIFIED



Year Group 2021

INTELLIGENCES: Logical-Mathematical, Spatial, Interpersonal

SKILLS: Cyber Corps officers are adaptive, collaborative, innovative, intellectually curious, and passionate leaders, capable of applying the art and science of the profession of arms within the cyberspace domain and electromagnetic spectrum (EMS) to plan, synchronize, integrate, and execute cyberspace and electronic warfare (EW) operations. They must be technically superior and technologically adept, understanding the cyberspace domain and EMS in a multi-dimensional sense to leverage leading-edge technologies and technically-skilled teams to provide operational commanders a unique effects-based capability for defending our nation against emerging threats. They must effectively articulate cyberspace and EW operational capabilities to commanders, as well as, integrate those capabilities to create effects during multi-domain operations in support of unified land operations at all echelons. They must also be lifelong learners to continue developing expertise as leaders in their field and to be highly adaptive within an emerging technological environment.

KNOWLEDGE: The Cyber Corps highly values officers with academic backgrounds in specific Science, Technology, Engineering, and Mathematics (STEM) disciplines and majors, but not exclusively. The domain-specific education disciplines listed below provide officers with a greater level of knowledge needed to plan, synchronize, and lead cyberspace operations. Other STEM and liberal arts disciplines and majors are also valued, but should be accompanied with demonstrated, cyber-related technical aptitude.

- **RELEVANT EDUCATION:** Computer Science/Engineering/Information Systems; Electrical Engineering; Mechanical Engineering; Cyber Security/Ops; Systems Engineering; Data Science; Mathematics; Physics; Chemistry; Information Technology/Systems/Security; Relevant STEM degree coupled with National/International Government, Policy, or Language Studies.
- **RELEVANT TRAINING / EXPERIENCE:** Cyber Leader Development Program; Cadet Troop Leading Time / Cadet Leader Development Time with cyber-related units; capture the flag events; technology or cyber conference participation; relevant cyberspace/ cybersecurity focused certifications; academic enrichment programs within academia, private sector, or government agencies.

BEHAVIORS:(In addition to foundational)

- | | | | | |
|-----------------------|------------------|--------------|----------------|-------------------|
| ➤ ADAPTABLE | ➤ DETAIL FOCUSED | ➤ EXPERT | ➤ INTELLECTUAL | ➤ PRECISE |
| ➤ COLLABORATIVE | ➤ DILIGENT | ➤ FLEXIBLE | ➤ INTEGRITY | ➤ PROBLEM SOLVING |
| ➤ CONFIDENT | ➤ DISCIPLINED | ➤ INITIATIVE | ➤ PASSIONATE | ➤ RESILIENT |
| ➤ CRITICALLY THINKING | ➤ ETHICAL/MORAL | ➤ INNOVATIVE | ➤ PERCEPTIVE | ➤ VISIONARY |

TALENT PRIORITIES:

1. **PROBLEM SOLVER:** Able to choose between best practices and unorthodox approaches to reach a solution. Accomplishes the task.
2. **INNOVATIVE:** Creative, inquisitive, and insightful. Easily identifies new solutions and catalyzes change.
3. **LOGICAL / ANALYTICAL:** Uses reason and thinks in terms of cause and effect. Able to deconstruct and solve complex problems.
4. **TECHNOLOGICALLY ADEPT:** Understands and effectively uses the latest technologies.
5. **INSPIRATIONAL LEADER:** Motivates teams to work harmoniously and productively towards a common goal.
6. **DOMAIN-SPECIFIC EDUCATION:** Possesses relevant academic disciplines desired by specific branch.



Branching Cyber



Minimum Requirements

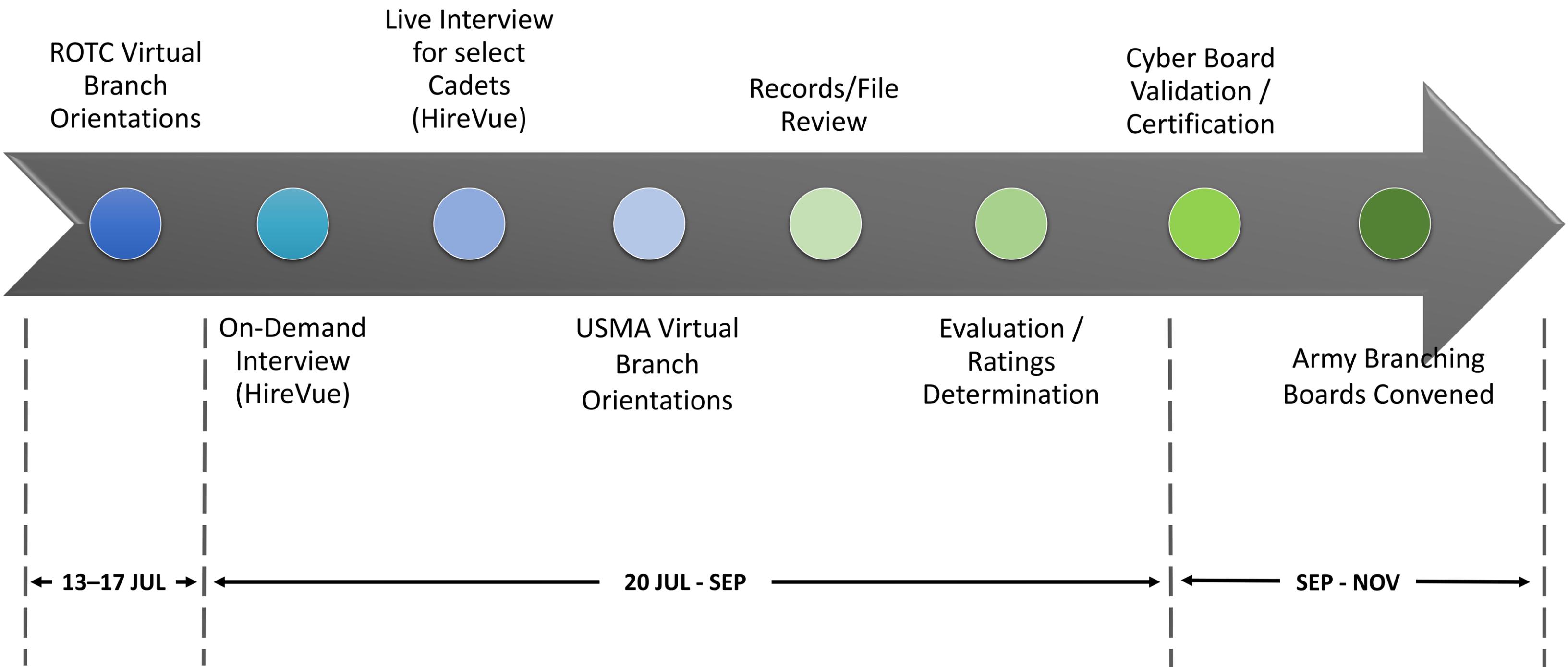
- Be a U.S. citizen
- Obtain and maintain TS/SCI clearance
- Pass CI-scope polygraph (as required)
- Pass “moderate” physical demands test
- Possess Bachelor’s Degree – specific STEM degree programs preferred, but not required
- Complete the Cyber Branch Assessment & Selection Process (aka the interview process) and **be selected** by Office, Chief of Cyber
- Be branched Cyber by the Army, ARNG, or USAR

Recommended Criteria

- Strong academic performer
- STEM degree program/track
- Cyber-related work experience, internships, fellowships, or volunteer work
- Cyber-related program participation (e.g., Cyber Leader Development Program)
- Cyber-focused academic project
- Cyber-related hobbies, interests, etc.
- Participation in Cyber challenges or competitions
- Recognized industry certifications (e.g., (ISC)2, CompTIA, EC-Council, SANS, etc.)
- Superior ROTC core skills rating/ranking



Branching Process Overview





Cyber Basic Officer Leaders Course

UNCLASSIFIED



Cyber BOLC = 36.85 weeks (9 months, 1 week)

**MODULE A
Common Core**

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
Cisco Certified Network Assoc.**

- Semester 1: Introduction to Networks
- Semester 1: Introduction to Networks Assessments
- Semester 2: Routing and Switching Essentials
- Semester 2: Routing and Switching Essentials Assessments
- Semester 3: Scaling Networks
- Semester 3: Scaling Networks Assessments
- Semester 4: Connecting Networks
- Semester 4: Connecting Networks Assessments

**MODULE C
Certified Information Systems Security Professional**

- CISSP Introduction
- Access Control
- Cryptography
- Telecommunications & Network Security
- Software Development Security
- Security Architecture & Design
- Business Continuity & Disaster Recovery Planning
- Physical Security
- Information Security & Risk Management
- Operations Security
- Legal, Regulations, Compliance & Investigations
- CISSP Review Assessment

**MODULE D
Python Scripting**

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

**MODULE E
Cyber Common Technical Core**

- Windows Command Line Tools
- Windows Processes
- Windows Registry
- Windows System Hardening Auditing and Logs
- Windows Networking
- Windows Tactical Survey
- Windows Final Exam
- Linux Core Features
- Linux Boot Processes
- Linux Scripts & Processes
- Linux Auditing & Logging
- Linux Exploitation
- Linux Capstone
- Linux Capstone/Exam Review
- Linux Final Exam
- Networking Fundamentals
- Network Reconnaissance
- Movement, Redirection & Data Transfer
- Watching the Wire
- Traffic Filtering
- Network Exploitation
- Industrial Control Systems (ICS)
- Networking Capstone
- Networking Review
- Final Exam

**MODULE F
Cyber Protection Team – Core Methodologies**

- Introduction
- CPT Overview
- CPT Overview Examination
- CPT Mission Planning
- Mission Planning Examination
- CPT Roles and Responsibilities During the Survey Stage
- CPT Survey Stage Examination
- CPT Roles and Responsibilities During the Secure Stage
- CPT Secure Stage Examination
- CPT Roles and Responsibilities During the Protect Stage
- CPT Protect Stage Examination
- CPT Roles & Responsibilities During the Recover Stage (w/ Guest Speaker)
- CPT Recover Stage Examination

**MODULE G
Cyber Operations Planners Course**

- Cyberspace Operations Framework
- Intelligence Support to Cyberspace Operations
- Offensive Cyberspace Operations Planning
- Defensive Cyberspace Operations (DCO)
- Administrative Lesson Plan
- Plan the Integration of Cyberspace Operations (Cortina STX)
- Cyberspace Operations Foundations Examination & Self Study
- Cyberspace Operations Guest Speakers (USG Agencies)

**MODULE H
Directed Self-paced Study**

- Online Training in Virtual Environment
- Penetration Testing with Kali Linux (PWK)
- Virtual Hacking Lab (VHL)



**MODULE I
Cyberspace Response Assessment (Capstone)**

- Week 1
 - Planning
 - Mission Protection
 - Discovery/Counter
 - Cyber Threat Emulation
 - Cyber Readiness
 - Cyber Support
- Week 2
 - Mission Commander
 - Analysis & Production
 - EA
 - ION

(Hands-on application of OCO and DCO skills)

- Graduation



UNCLASSIFIED



Cyber & Electronic Warfare Officer Qualification Course

UNCLASSIFIED



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

<p>MODULE A Introduction</p> <ul style="list-style-type: none"> •Course orientation •Army EW Vision •Duties & Responsibilities •Security briefing •Pre-test 	<p>MODULE B Electronics Theory</p> <ul style="list-style-type: none"> •Math for CEWOs •Theory and principles of electricity •Into to the EMS •Radio Wave fundamentals •Radio Wave propagation •Exam 	<p>MODULE C Comms Systems</p> <ul style="list-style-type: none"> •Army, Joint, Allied comms systems •Cellular communications •Exam 	<p>MODULE D EMS Based Systems</p> <ul style="list-style-type: none"> •Fundamentals of Radar •Characteristics of Electro-Optics •GPS & PNT •C-UAS Systems •Exam 	<p>MODULE E Electronic Attack</p> <ul style="list-style-type: none"> • 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 	<p>MODULE F Electronic Warfare Support</p> <ul style="list-style-type: none"> •ES Authorities •National SIGINT request process •Deconflict ES & SIGINT •ES Systems •ISR Platforms and Support •Exam 	<p>MODULE G Electronic Protection</p> <ul style="list-style-type: none"> •Spectrum Management Doctrine • EM Hardening & Shielding •EMCON •Emission deconfliction •Friendly C2 systems and sensor vulnerabilities •Degrade Operations •Deception TTPs •S2AS EME Survey •Exam 	<p>MODULE H CEMA Support to Operations</p> <ul style="list-style-type: none"> •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 	<p>MODULE I Plan CEMA Support to Operations</p> <ul style="list-style-type: none"> • 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 	<p>MODULE J EW Ground Operations</p> <ul style="list-style-type: none"> •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 	<p>MODULE K Culminating Event</p> <ul style="list-style-type: none"> • FTX • Graduation
---	--	--	--	---	--	---	--	--	---	--



UNCLASSIFIED



Cyber Capabilities Development Officer BOLC

UNCLASSIFIED



17D BOLC = 47 weeks (10 months, 3.5 weeks)

**MODULE A
Common Core**

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
Technical Introduction**

- Reverse Engineering Concepts
- Developer Project Assignment



**MODULE C
Technical Core**

- Course Integration
- Networking
- Discrete Math
- Python Programming I
- Python Programming II
- X86 Assembly

- Network Programming in C
- Culminating Event x 5
- Intro to C Programming
- Intermediate C Programming
- Data Structures and Algorithms I
- Data Structures and Algorithms II

- Object-Oriented Python
- Operating Systems
- Network Programming in Python
- Intro to Cryptography
- Organizational Processes

**MODULE D
Culminating Activities**

- Developer Project Completion/ Evaluation
- Qualification Event (4 weeks)
- Job Qualification Requirements Completion
- Graduation



Pending Final Army Approval of AOC 17D

UNCLASSIFIED

What to Expect as a Cyber Lieutenant



17A Cyber Warfare Officer

- Cyber Defense Manager
- Cyber Section Leader
- Cyber Planner
- Cyber Operator/Analyst



17B Cyber & Electronic Warfare Officer

- Platoon Leader
- Cyber/CEMA Planner
- Unit CEWO
- Company XO



17D Cyber Capabilities Development Officer

- Basic Developer
- Developer Team Member

A day in the life of a Cyber Lieutenant consists of...

Training & planning for cyberspace operations
 Performing & supervising technical analysis
 Executing & supervising interactive operations
 Certifying in Cyber work roles

Training & planning for Electronic Warfare missions
 Performing & supervising equipment maintenance
 Advising the Commander on Cyber/EW capabilities
 Deployments & TDY missions

Developing Cyber/EW capabilities
 Specialized training/certifications
 Leadership & staff duties
 Physical fitness & Army training

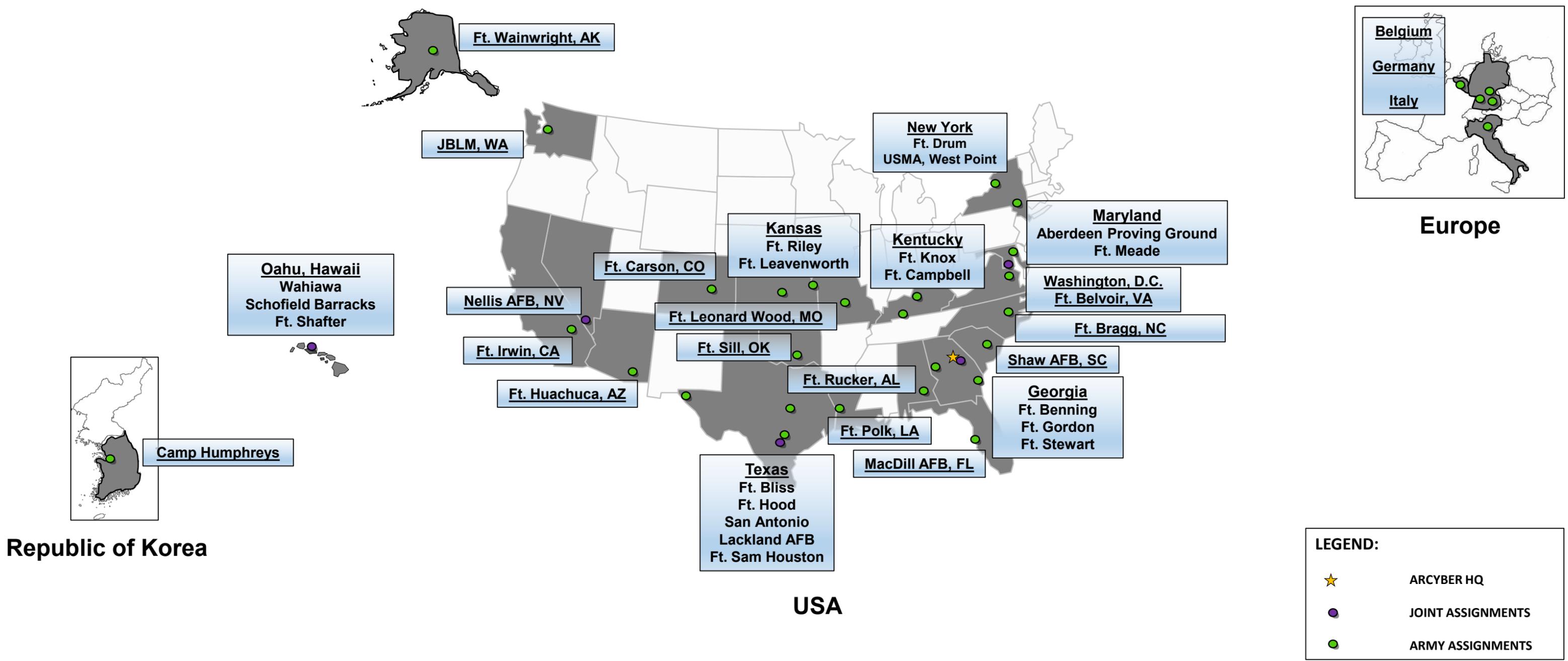


Cyber Corps Duty Locations

UNCLASSIFIED



Active Component



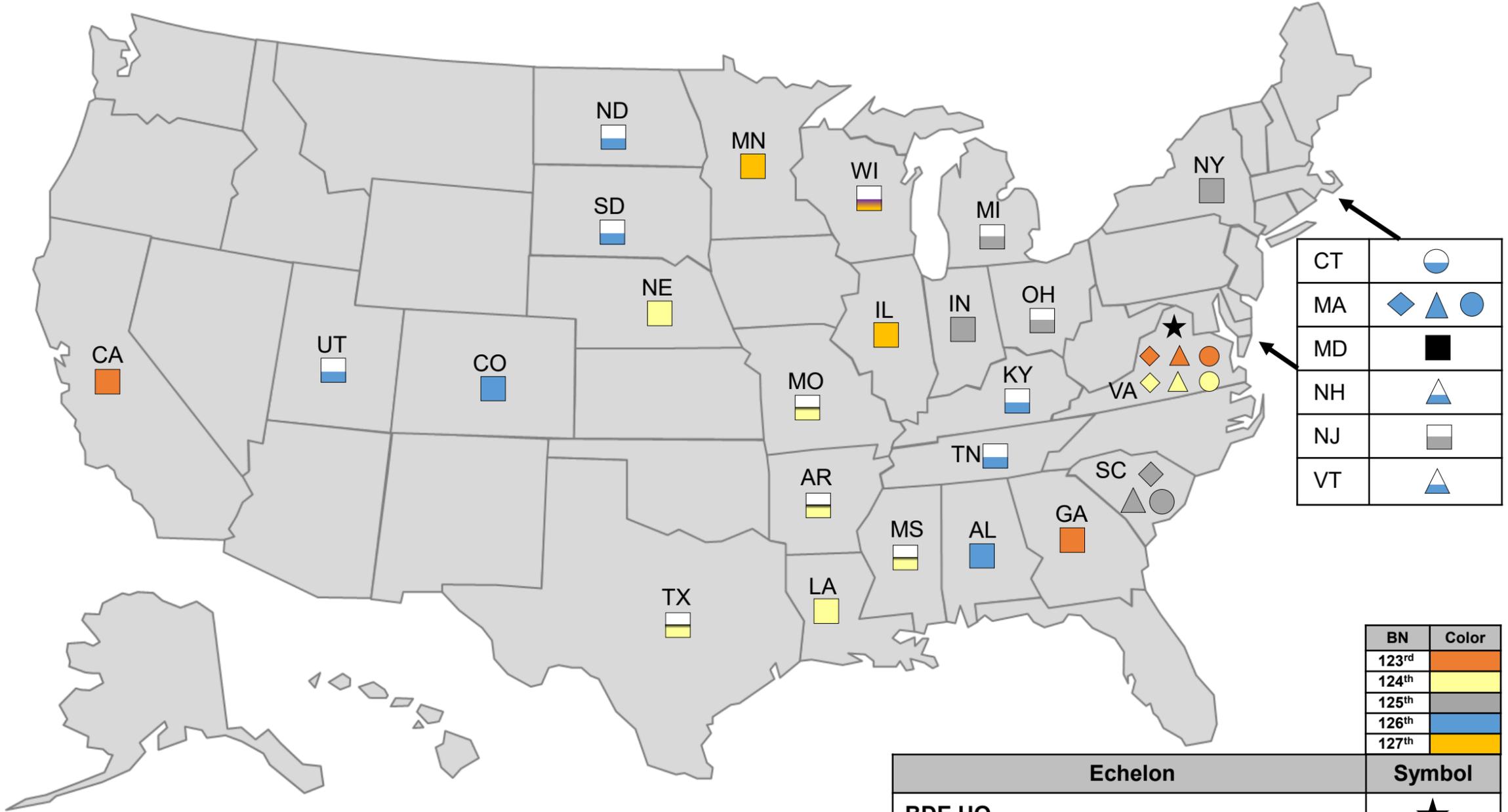
Republic of Korea



Army National Guard Cyber Units

91st Cyber Brigade

UNCLASSIFIED

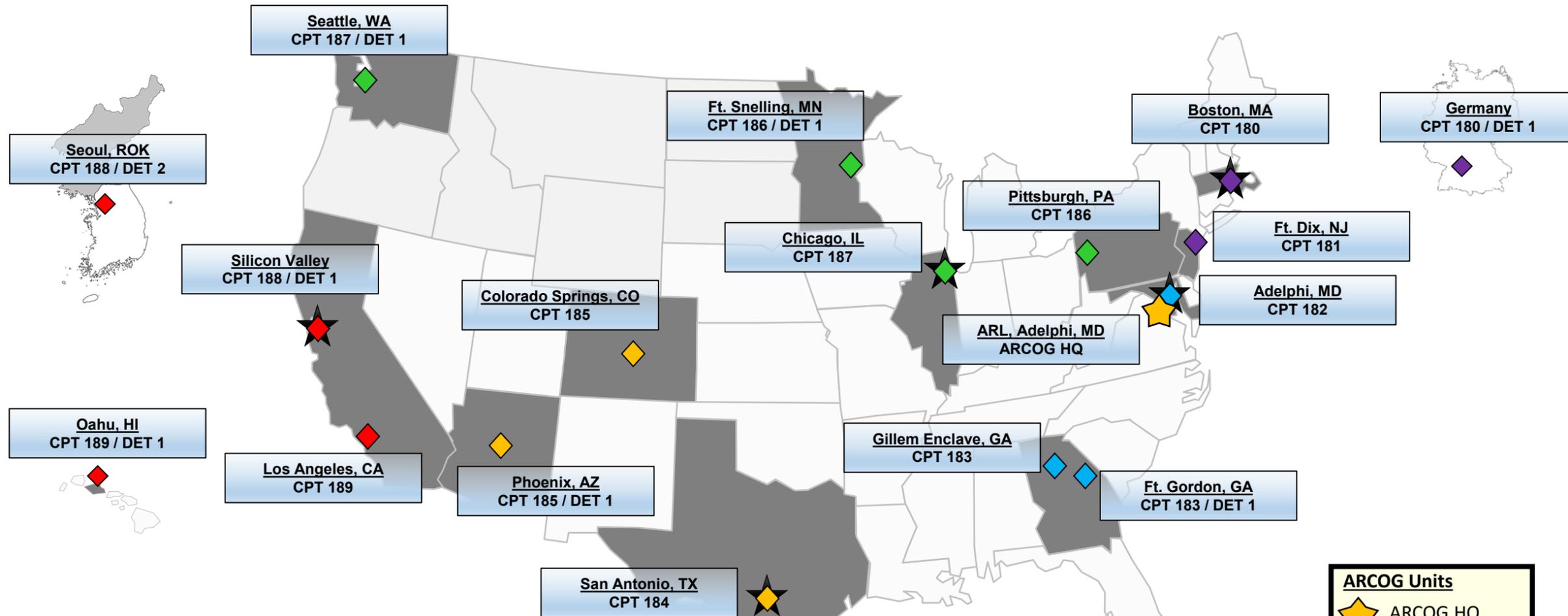


CT	
MA	
MD	
NH	
NJ	
VT	

BN	Color
123 rd	
124 th	
125 th	
126 th	
127 th	

Echelon	Symbol
BDE HQ	
BN HQ	
Cyber Security Company (CSC) HQ / Det	
Cyber Warfare Company (CWC) HQ / Det	
Cyber Protection Team (CPT) HQ / Det	

U.S. Army Reserve Cyber Units



ARCOG Units

- ARCOG HQ
- NCR CPC
- NE CPC
- NC CPC
- SW CPC
- W CPC
- BN HQ

CPC = Cyber Protection Center

Points of Contact



Cyber Branching Site:

https://oema.army.mil/branching_public/index.htm

Select "CY"

OCC Officer Division Mailbox:

usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil

Officer Division Chief: Mr. Phillip Williams, phillip.e.williams.civ@mail.mil

Force Integration Specialist: Ms. Montrese Love, montrese.r.love.civ@usa.army.mil

17A Career Program Manager: CPT Antonia Feffer, antonia.l.feffer.mil@usa.army.mil

17B Career Program Manager: MAJ Kyle Borne, kyle.d.borne.mil@usa.army.mil



USAR Representative: LTC Michael Orlandella, michael.a.orlandella.mil@usa.army.mil

ARNG Representative: MAJ Danny Kang, danny.g.kang.mil@usa.army.mil

