FIGHT THROUGH THE ATTACK

THE CYBER SECURITY FORUM INITIATIVE

WWW.CSFI.US

CSFI CYBERSPACE OPERATIONS TRAINING

"Our CSFI courses are endorsed by Capitol Technology University (CTU), a designated National Security Agency (NSA) Center of Excellence."

LIVE ONLINE AND ONSITE

CYBERSPACE OPERATIONS

TRAINING CAREER PATH RECOMMENDATION

Introduction to Cyber Warfare and Operations Design (ICWOD)

Learn the core set of skills needed to design and plan for cyberspace operations at all levels of the planning spectrum.

COURSE OVERVIEW:

This course provides a basic understanding of full-spectrum cyberspace operations; the complexities of the cyberspace environment; and planning, organizing, and integrating cyber ops. The course consists of presentations and exercises that teach students how to design a cyberspace operations plan and bring it to fruition. Presented with an international conflict scenario, students are guided through a series of cascading exercises for conceptual, functional, and detailed planning. Following the design concept for problem framing students utilize the commander's intent to plan toward the desired end state. At course conclusion, students will have an appreciation for the planning process and have a fundamental understanding of how to plan for and cyberspace operations. This course in endorsed by Capitol Technology University (CTU), a designated National Security Agency (NSA) Center of Excellence.

YOU WILL LEARN:

- Understanding the Cyberspace Environment and Design
- Cyberspace Strategies
- Cyberspace Operations
- Cyberspace Operations Integration
- Building Cyber Warriors and Cyber Corps
- Designing Cyber Related Commands
- Training and Readiness for Cyber Operations
- Rehearsal of Concept (ROC) Drill
- Tabletop Exercise (TTX)

IS THIS THE RIGHT COURSE?

Developed exclusively for the Cyber Security Forum Initiative (CSFI) by professionals with experience in military cyberspace operations, this course provides an introduction to cyber operations in the context of cyber warfare and the accompanying planning process. While this course includes a military scenario and doctrine, the concepts learned can be applied to virtually any organization with a cyber environment.

CSFI is highly invested in protecting American national security in cyberspace and is proud to provide cyberspace operations training to American entities, as well as foreign allies and partners in support of interoperability.

While not a prerequisite, students of this course would benefit by having a basic understanding of cyber fundamentals.

COURSE OUTLINE:

Understanding the Cyberspace Environment and Design

- Defining cyberspace
- Design
- Environmental Frame
  - Layers of Cyberspace
  - OSI Model
  - Cyberspace & the Warfighting Funtions & the Elements of Combat Power
- Problem Framing
- Operational Approach
- Planning Power Words

Cyberspace Operations

- Defining Cyberspace Operations
  - Network Operations (NetOps)
  - Defensive Cyberspace Operations (DCO)
  - Offensive Cyberspace Operations (OCO)
- Operations Models
  - Westphalian Model
  - Global Commons Model
  - Tallinn Manual
  - Operational Methodologies

Building Cyber Warriors and Cyber Corps

- Warrior and Warrior Corps Concept
- Cyber Warrior and Cyber Corps Concept
- Posturing the Cyber Workforce

Cyberspace Strategies

- Operating Networks
  - Information Assurance
- Defending Networks
  - Network Security
  - Proactive Defense/Hunting
  - Intelligence Driven CND
  - Intelligence Driven CND Case Study
- Cyberspace Operational Methodologies
  - Warfighting Domain
  - Enabling Operation
  - Supporting Operation

Cyberspace Operations Integration

- Intelligence-Driven Cyberspace Operations
- Intent Behind Cyberspace Operations
- Cyberspace Operations Fusion
- Cyberspace Operations as a Supporting
- Function
- Cyber Unity of Effort Example
- Cyber Integration into Joint Operations,
- Example
- Scenario

Rehearsal of Concept (ROC) Drill

Tabletop Exercise (TTX)

Training and Readiness for Cyberspace Operations

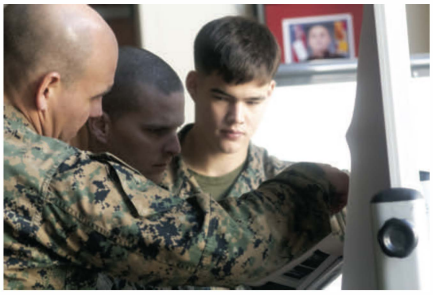
- Readiness Concept
- Mission Essential Tasks (METs)
  - Subordinate Tasks/Battle Tasks
- Training for Unit Operations
- Exercise Planning
- Sustaining Readiness

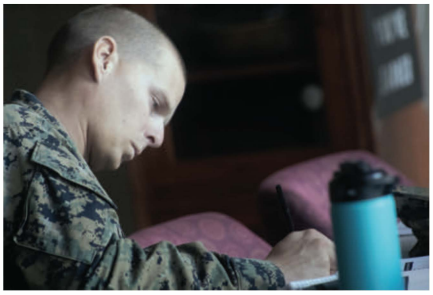
Designing Cyber Related Commands

- Understanding the Operating Environment
- Tasks to Functions Alignment
- Building Task Organizations
  Levels of Planning
  - Conceptual
  - Functional
  - Detailed

ICWOD GROUP LABS:

- Exercise 1: Problem Framing and Operational Design
- Exercise 2: Strategy Development
- Exercise 3: Cyberspace Operations Development
- Exercise 4: Cyberspace Operations Integration
- Exercise 5: Command Design
- Exercise 6: Mission Essential Task Development
- Rehearsal of Concept (ROC) Drill
- Tabletop Exercise (TTX)
- Capstone Report





The Cyber Security Forum Initiative (CSFI) is proud to train MAWTS-1 (MARINE AVIATION WEAPONS AND TACTICS SQUADRON ONE).

DEFENSIVE CYBERSPACE OPERATIONS ENGINEER (DCOE)

CERTIFICATION

CSFI Trains and Certifies MITRE/USAF in Los Angeles.

Develop your cyberspace operations skills for the deployment of NETOPS, DCO, and OCO.

COURSE OVERVIEW:

Students will develop the skills for executing defensive cyberspace operations (DCO) into organizational missions. Adversarial tactics, techniques, and procedures (TTPs) and associated tools are presented following the cyber kill chain for students to learn to defend friendly networks against current and emerging threats. Using multiple labs, this course provides students withhands-on exposure to deploy live attacks and analysis in a controlled environment to then learn how to prevent, detect, and counter such activities.

The DCOE training provides a unique opportunity to certify in a critical field of cyberspace operations,enhanching mission readiness and employability. The DCOE certification follows the NICE work role and standards for a Cyber Operator.

This course in endorsed by Capitol Technology University (CTU), a designated National Security Agency (NSA) Center of Excellence.

YOU WILL LEARN:

- Cyberspace Operations and Cyber Mission Force
- Cyber Kill Chain
- Kali Linux
- Reconnaissance (Passive and Active)
- PBED for Cyberspace Operations
- Attack Across Networks and Systems
- Persistent, Integrated Operations
- Network Protection

CSFI-DCOE

IS THIS THE RIGHT COURSE?

Developed exclusively for the Cyber Security Forum Initiative (CSFI) by professionals with experience in military cyberspace operations, this course is designed to help students acquire knowledge and appreciation of preserving the ability to protect data, networks, net-centric capabilities, and mission critical systems.

CSFI is highly invested in protecting American national security in cyberspace and is proud to provide cyberspace operations training to American entities, as well as foreign allies and partners in support of interoperability.

While not a prerequisite, students of this course would benefit by having a working knowledge of TCP/IP, at least one year of IT security experience, and completed the CSFI Introduction to Cyber Warfare and Operations Design (ICWOD) course.

COURSE OUTLINE:

Introduction

- Certification Requirements
- Commander's Intent
- Evolution of Cyber Espionage and Collection Efforts

PBED for Cyberspace Operations

- PBED Framework
- Plan – ME3C-(PC)2 Model
- Brief
- Execute
- Debrief
- PBED Exercise

Kali Linux

- Cyber Tradecraft
- Installation

CSFI Cyberspace Operations Planning Session, California

Cyberspace Operations and Cyber Mission Force

- Cyberspace as a Warfighting Domain
- The Operating Environment
- Cyberspace Militarization
- DOD Cyber Strategy
- Cyberspace Operations
  - NetOps, DODIN Ops
  - DCO (DCO-IDM, DCO-RA)
  - OCO
- CMF Construct – CPT, NMT, CMT
- CPT Methodology (Survey, Secure, Protect)

Attack Across Networks and Systems

- Web Application Vulnerabilities
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Webshell
- Wireless Threats
- Network Exploitation
- Conducting Attacks with Metasploit
- Password Cracking

Cyber Kill Chain

- Steps of the Cyber Kill Chain
- Stages of an Attack
- Case Study: Data Breach and Lessons Learned
- Threat Intelligence Sharing

Persistent, Integrated Operations

- Command and Control (C2): Maintaining Access
- Rootkits
- Tunneling
- Remote Access
- Elevated Privileges
- Covert Channels
- Covering Tracks: Hiding Evidence
- Altering Logs and History Files
- Hidden Files
- Timestamps

Reconnaissance (Passive and Active)

- CIA's MICE Motivational Framework
- Open Source Intelligence (OSINT) – Common Tools
- Information Sources
- Case Study: Social Media Experiment
- Reconnaissance with Kali Linux
- Network Scanning
- SQL Mapping

Persistent, Integrated Operations

- Network Traffic Analysis
- Vulnerability Scanning
- Intrusion Detection System (IDS) and Intrusion
- Protection System (IPS)

DCOE HANDS-ON LABS:

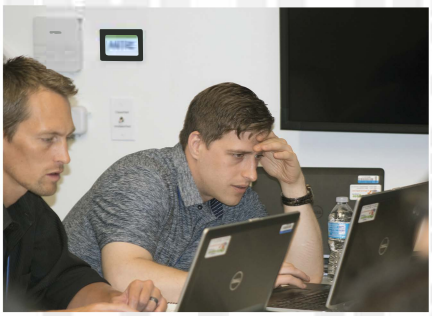
- Lab 01: Navigating Kali Linux
- Lab 02: Network Mapping
- Lab 03: Python Scripting: Scanning and Brute Force
- Lab 04: PBED Exercise
- Lab 05: Cracking Wireless
- Lab 06: Metasploit 1
- Lab 07: Metasploit 2
- Lab 08: Metasploit 3
- Lab 09: EternalBlue (Shadow Brokers)
- Lab 10: SQL Injection
- Lab 11: Password Cracking
- Lab 12: Data Exfiltration
- Lab 13: Kernel Rootkit
- Lab 14: Packet Capture and Analysis
- Lab 15: IDS Deployment, Alert Analysis, and Reporting
- Bonus Lab: Vulnerability Scanning
- Bonus Lab: OSINT and Malware Analysis: Syrian Electronic Army (SEA)
- Bonus Lab: Whispergate Malware Analysis - Destructive Malware Targeting Ukrainian Organizations and Government.
- CAPSTONE: Capture-the-Flag (CTF)
- And more !

Certified CSFI DCOE Instructor facilitating cyberspace operations planning.

USAF Cyber Warfare Operations DCOE-ICWOD training MITRE on PBED.

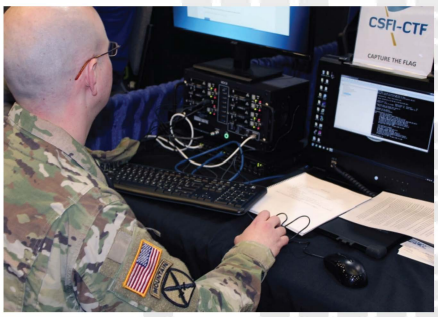
CSFI trains and certifies the Social Security Administration DCOEs.

CSFI DCOE (Defensive Cyberspace Operations Engineer) training.



CSFI DCOE CTF Exercise.

CSFI DCOE Fly Away Kit – Cyber Ops Capabilities.



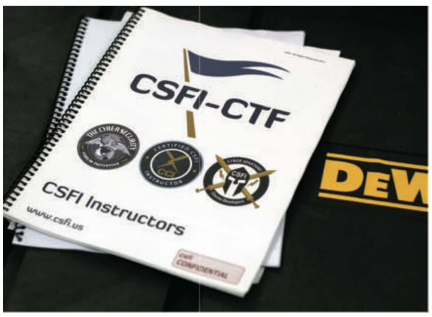
CSFI DCOE CTF Cyber Challenge.

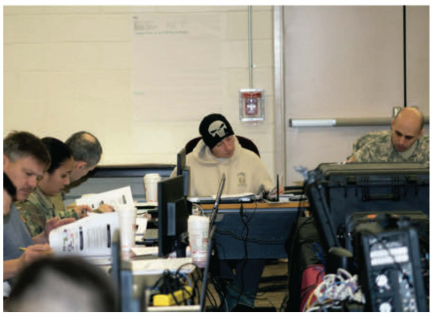
DCOE Students plan for cyber-space operations . Great ICWOD exercise.

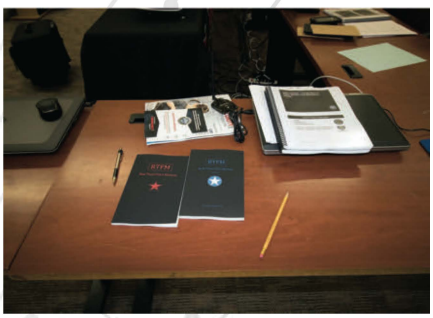
CSFI DCOE CTF (Capture The Flag) Cyber Challenge.

CSFI TRAINS AND CERTIFIES

THE NEW JERSEY NATIONAL GUARD AS DCOES



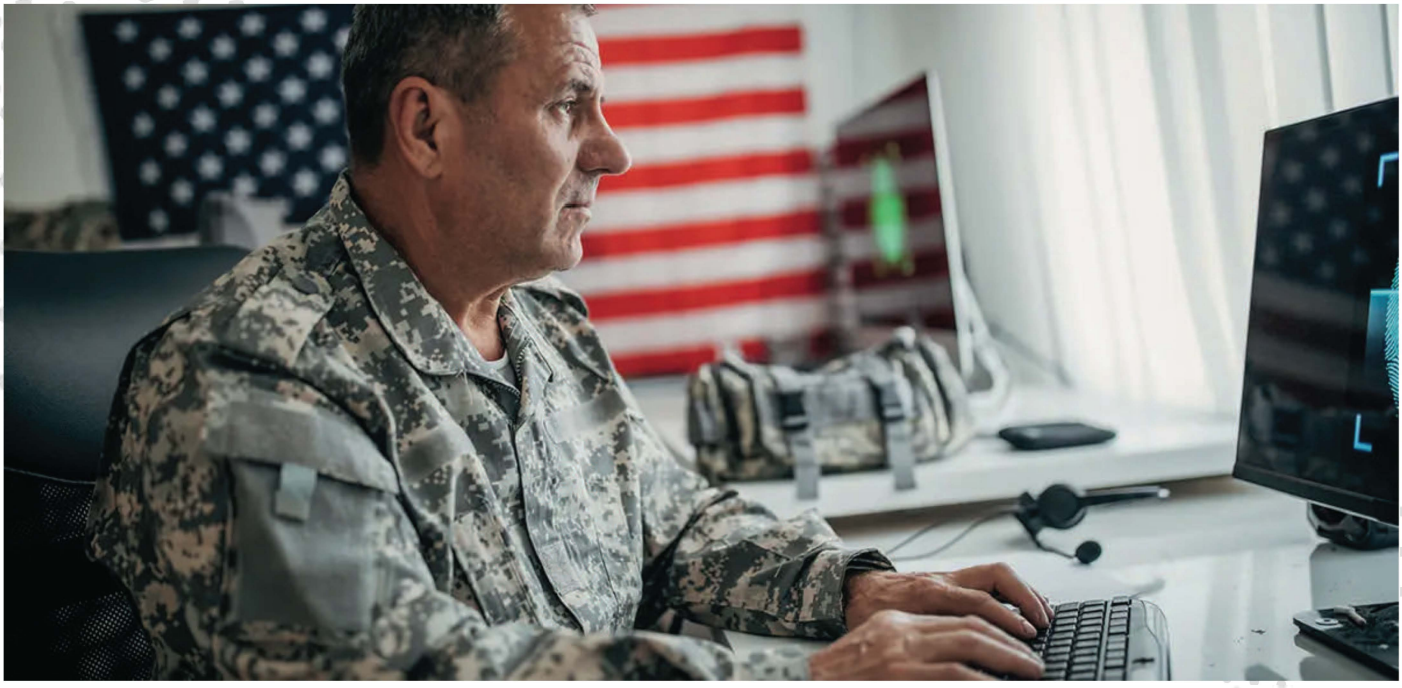




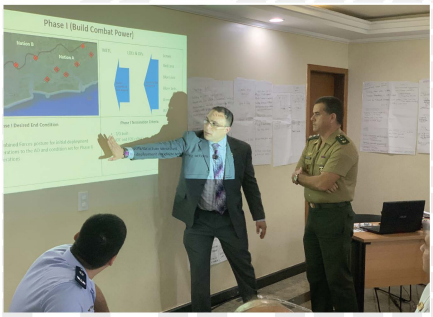
OPERATIONS

CSFI STANDARDS

CSFI only trains and certifies clients in accordance with American national security interests.



CSFI was honored to provide the *Cyberspace Operations Planning Training* course to the Fórum Ibero-Americano de Defesa Cibernética in partnership with the Brazilian Cyber Command. A special thank you to all who worked very hard to make this highly qualified Cyber Ops training event a success. Thank you, Brazil, Argentina, Colombia, Spain, Portugal, Mexico, and Uruguay for your participation and dedication during this intense cyberspace operations planning exercise. A special thank you to the Brazilian Federal Police and the Gabinete de Segurança Institucional da Presidência da República, GSI.



TESTIMONIALS

Mark Kelton

CSFI Advisory Director; former Deputy Director of the National Clandestine Service for Counterintelligence,Central Intelligence Agency (CIA).

"The Cyber Security Forum Initiative (CSFI) is unique in its mission of maintaining and furthering those advantages by fostering Cyber awareness and collaboration among the U.S. government, military and commercial sectors, as well as with international partners."

Michael Groen

LtGen. (Ret.), USMC; Former Director of the Joint Artificial Intelligence Center, DOD, former Deputy Chief of Computer Network Operations of the National Security Agency (NSA), CSFI Advisory Director.

"ARE YOU ON THE RIGHT COURSE? Check out CSFI's Operations Design course that puts Cyber Operations (DCO, OCO) into a contingency context. Thought-provoking content."

USMC Lt Gen (ret.) John Toolan

CSFI Advisory Director; former Commander of the 2nd Marine Division.

"The reputation of CSFI particularly in the area of cyber and the information environment is stellar."

USAF Maj Gen (ret) Harold "Punch" Moulton

CSFI Advisory Director; former Director of Operations, US European Command.

"As a strategist for cyberspace, I rely on keen insights and focused information. I turn to CSFI daily."

Sean P. Roche

CSFI Advisory Director; former Associate Deputy Director of the Central Intelligence Agency (CIA) for Digital Innovation.

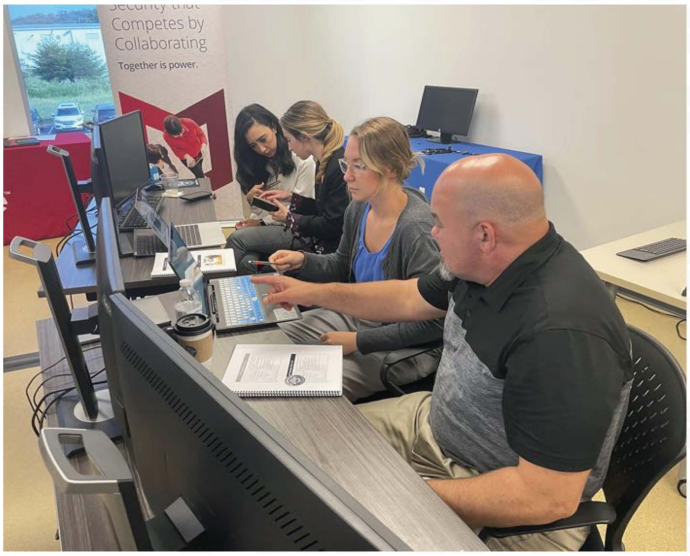
"In a world that competes for your time and attention CSFI is high payoff."

CSFI CLIENTS

"Progress Is Only Possible If The United States And Its Allies Work Together."

- Brent Scowcroft
Former United States
National Security Advisor.

OFFICE AND TRAINING FACILITIES



QUANTICO OFFICE

Training Facility
1010 Corporate Drive
Stafford, VA 22554

TRAINING FACILITY (VIRGINIA BEACH)

2829 Guardian Lane
Suite 150
Virginia Beach, VA 23452

MANASSAS HISTORIC DISTRICT OFFICE

9401 Battle St.
Suite 202
Manassas, VA 20110

Cyber Security Forum Initiative, Inc. (CSFI)
9401 Battle Street, Suite 202 Manassas, VA 20110, USA
www.csfi.us
CAGE CODE 8L7W