NATIONAL CYBER DEFENSE MANDATE

Mastery in Cyber Warfare
Training and Education

An elite non-profit providing the operational insight and technical capability required to achieve integrated deterrence across the cyber domain. Supporting the American warfighter, the U.S. Government, and our allies through training, education, and services.

700K+	4	DCWF	GSA
GLOBAL MEMBERS	TACTICAL CERTIFICATIONS	FRAMEWORK ALIGNED	MAS CONTRACT HOLDER

WWW.CSFI.US

THE ORGANIZATION

Cyber warfare awareness, guidance, and solutions.

The Cyber Security Forum Initiative is a non-profit organization and a community of more than 700,000 cyber security and cyber warfare professionals, founded on March 6, 2009 by Dr. Paul de Souza.

700K+	2009	3	4
MEMBERS WORLDWIDE	YEAR FOUNDED	HEADQUARTERS IN VIRGINIA	SECTORS UNITED

> "To provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

THE CSFI MISSION · DR. PAUL DE SOUZA, FOUNDER AND PRESIDENT

BUILT BY A COMMUNITY, ACROSS FOUR SECTORS

01
Government
Agencies and public servants defending national interests in cyberspace.

02
Military
Service members and units on the front lines of cyber operations.

03
Private sector
Companies and practitioners protecting commercial and critical systems.

04
Academia
Researchers, faculty, and students advancing the field.

COLLABORATION IS THE FOUNDING PRINCIPLE OF CSFI

WHY CSFI EXISTS

Supporting the American warfighter in cyberspace.

Through cutting edge training, target development frameworks, and public private operational collaboration, CSFI enhances the readiness and systemic resilience of military, government, and allied networks to defend forward and neutralize sophisticated nation state threats.

FIELD CYBER OPERATIONS

READINESS · RESILIENCE · DETERRENCE

TOTAL FORCE

CSFI supports USCYBERCOM in retaining Cyber Mission Force work roles across the Total Force.

FRAMEWORK

Certification pipelines map directly to the Department of War Cyber Workforce Framework, so partners can place graduates straight into force development plans.

U.S. Department of War

DCWF · U.S. DEPARTMENT OF WAR

ALLIES AND PARTNERS

Interoperability is the point.

CSFI is highly invested in protecting American national security in cyberspace, and provides cyberspace operations training to American entities as well as to foreign allies and partners in support of interoperability. Programs are delivered across NATO member nations and major non-NATO allies.

CSFI is a privately owned, independent non-profit. It is not part of, and does not represent, any U.S. Government agency or any other governmental entity.

UNITED STATES

NATO OTAN

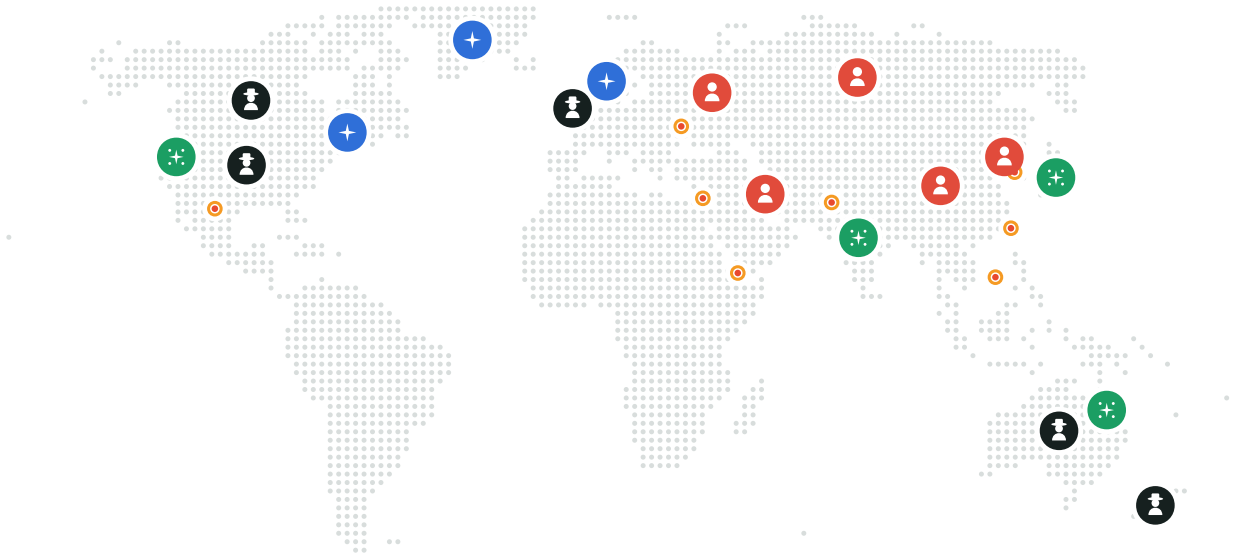
NORTH ATLANTIC TREATY ORGANIZATION

WHY THE MISSION MATTERS

The New Cold War is Hybrid

A convergence of threats across geopolitical, cyber, and physical domains

GEOPOLITICAL · CYBER · PHYSICAL



Geopolitical hot spots

- Ukraine / Russia
- Israel / Palestine
- Taiwan Strait
- South China Sea
- DPRK / ROK
- India / Pakistan
- The Red Sea (Bab el-Mandeb Strait)
- Southern US border

Rogue cyber actors

- People's Republic of China
- Russia
- Iran
- North Korea

Key US alliances / security partners

- The Five Eyes (US, UK, CA, AU, NZ)
- NATO (32 members across Europe & US)
- Quad (Australia, India, Japan, US)

A former Office of Naval Research (ONR) Science Advisor talks about the rigorous CSFI CyberOps training course that will help you succeed in your cyber career.

Dr. Roger W. Kuhn Jr. · CSFI Advisory Director · former ONR Science Advisor

CERTIFIED TRAINING MODULES

Four certifications. One operational pipeline.

Rigorous certification pipelines that prepare security personnel for highly complex digital engagements, developed by professionals with experience in military cyberspace operations.

CERTIFICATION	CODE	LEVEL	DURATION AND DELIVERY	CREDENTIAL
ICWOD Introduction to Cyber Warfare and Operations Design	CSFI-01	Foundational	On-demand, self-paced	Certificate
DCOE Defensive Cyberspace Operations Engineer	CSFI-02	Specialist	Live, online, or asynchronous	Certification
CTDA Cyber Target Development Analyst	CSFI-04	Advanced	Three days, all formats	Certification
CCTI-A&S Certified Cyber Threat Intelligence Analyst and Strategist	CCTI	Analyst and Strategist	Five days, 40 hours, instructor-led	Certification

THE PIPELINE

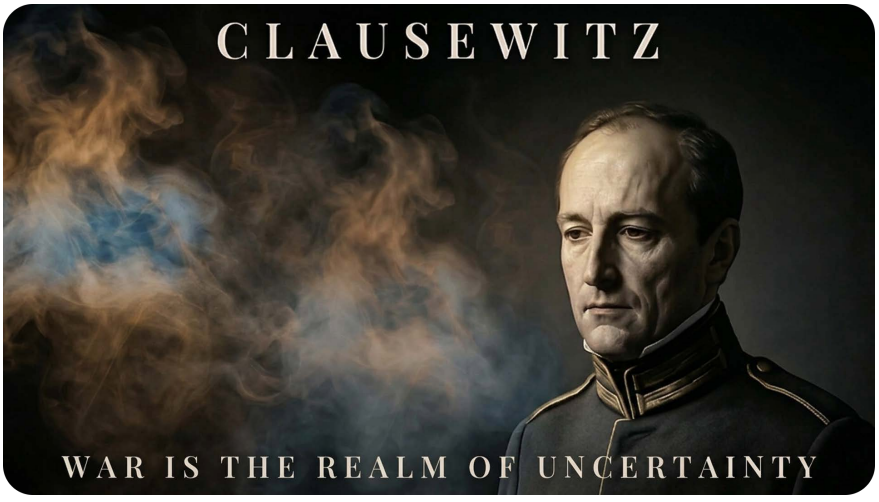
ONE SEQUENTIAL PATH · STEPS 01 TO 04

STEP 01 · START HERE
ICWOD
Plan and design cyberspace operations. A demanding foundation, and the baseline every track builds on.

STEP 02 · DEFEND
DCOE
Hands-on defensive operations. NetOps, DCO, and OCO across 15 labs.

STEP 03 · TARGET
CTDA
Joint targeting doctrine applied to the cyber domain. Prerequisite: ICWOD.

STEP 04 · SPECIALIST
CCTI-A&S
Cyber threat intelligence tradecraft, from requirements to finished reporting.



WHY START WITH ICWOD

Foundational. Not easy.

ICWOD is the entry point, and it is demanding by design. Students plan cyberspace operations through cascading conceptual, functional, and detailed design exercises, graded to the standards working cyber warfare planners are held to.

Foundational means first, not light. It is the qualification every CSFI track builds on.

THE SIX PHASE JOINT TARGETING CYCLE · JP 3-60

Doctrine drives the pipeline.

CSFI training is anchored to the joint targeting cycle. CTDA concentrates on Phase 2, where targets are developed and prioritized for operations in and through cyberspace.

PHASE 1
End state and commander's objectives

PHASE 2 · CTDA FOCUS
Target development and prioritization

PHASE 3
Capabilities analysis

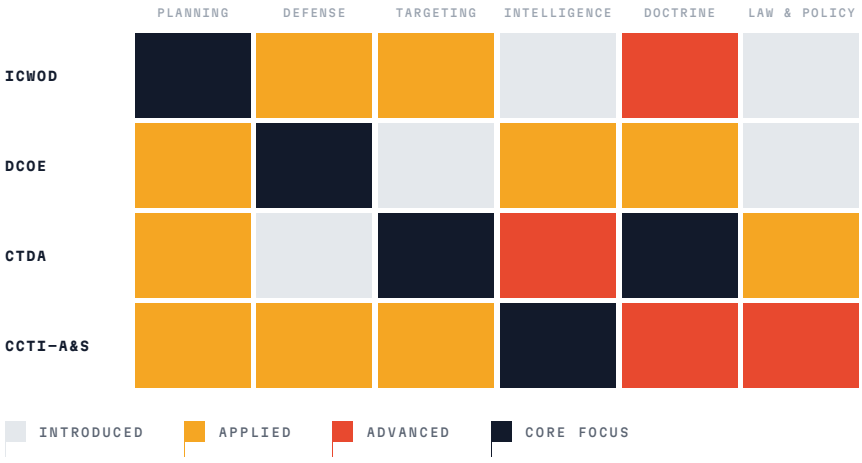
PHASE 4
Commander's decision and force assignment

PHASE 5
Mission planning and force execution

PHASE 6
Assessment

MISSION COVERAGE HEAT MAP

Depth of coverage, by certification.



HOW TO READ IT

Every track begins from the same planning foundation, deepens in its own mission area, and converges on the DCWF so graduates slot directly into force development plans. Coverage depth reflects each course's published curriculum.

6
PHASES IN THE TARGETING CYCLE

4
CERTIFICATIONS, ONE PIPELINE

6
MISSION AREAS COVERED

4
DEPTH LEVELS, INTRODUCED TO CORE

OPERATIONS DESIGN CONCEPTUAL · FUNCTIONAL · DETAILED

MODULE CSFI-01 · ICWOD

Introduction to Cyber Warfare and Operations Design

Learn the core set of skills needed to design and plan for cyberspace operations at all levels of the planning spectrum. Presented with an international conflict scenario, students move through cascading exercises for conceptual, functional, and detailed planning.

CYBERSPACE PLANNING | ROC DRILL | TABLETOP EXERCISE | CAPSTONE

COURSE AT A GLANCE	
FORMAT	100% on-demand
ACCESS	Computer, phone, tablet
LABS	6 exercises, ROC, TTX
CREDENTIAL	ICWOD certificate
ENDORSED BY	Capitol Tech University

DEMANDING BY DESIGN

Foundational in scope, professional in rigor. Built for cyber warfare planners and graded to real planning standards.

EIGHT CORE COMPETENCIES

01
The Cyberspace Environment and Design
Frame the operating environment, the layers of cyberspace, and the OSI model as the foundation for operational design.

02
Cyberspace Strategies
Operate, defend, and secure networks through intelligence driven, proactive defense and hunting methodologies.

03
Cyberspace Operations Integration
Fuse intelligence and commander's intent to integrate cyber effects into joint operations.

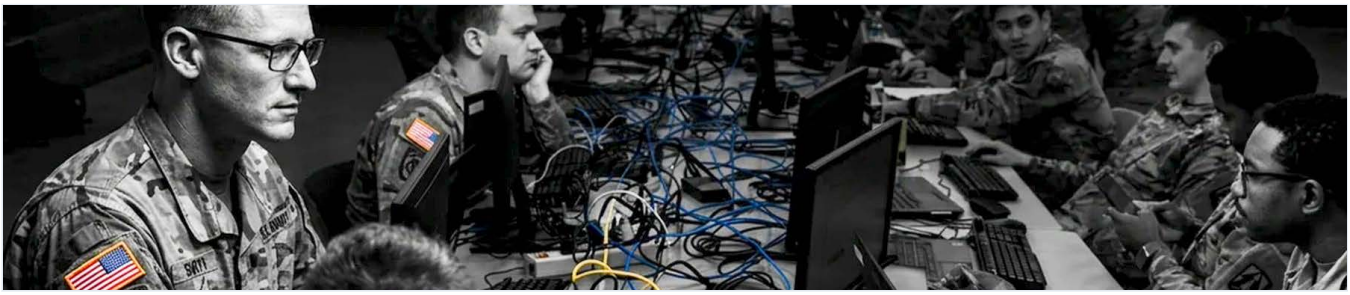
04
Building Cyber Warriors and Cyber Corps
Apply the warrior corps concept to posture, build, and develop the cyber workforce.

05
Designing Cyber Related Commands
Translate environment understanding into task organizations across every level of planning.

06
Training and Readiness
Develop mission essential tasks and sustain readiness through deliberate exercise planning.

07
Rehearsal of Concept Drill
Walk the plan end to end to validate synchronization before execution.

08
Tabletop Exercise
Stress test decisions against a live scenario to refine the operational approach.



DEFENSIVE CYBER OPERATIONS NETOPS · DCO · OCO

MODULE CSFI-02 · DCOE

Defensive Cyberspace Operations Engineer

Adversarial tactics, techniques, and procedures are presented following the cyber kill chain, so students learn to defend friendly networks against current and emerging threats. Multiple labs give hands-on exposure to live attacks in a controlled environment.

CYBER KILL CHAIN | KALI LINUX | LIVE ATTACK LABS | IDS AND IPS

COURSE AT A GLANCE	
FORMAT	Live, online, async
LABS	15 hands-on, 3 bonus
DCWF ROLE	Cyberspace Operator
ELEMENT	Cyberspace Effects
WORK ROLE ID	322

EIGHT CORE COMPETENCIES

01
Cyberspace Operations and Cyber Mission Force
Frame cyberspace as a warfighting domain and the CMF construct across NetOps, DCO, and OCO.

02
Cyber Kill Chain
Trace every stage of an attack and apply threat intelligence sharing through real breach case studies.

03
Kali Linux
Build cyber tradecraft on Kali Linux: installation, command line tasks, and confident navigation.

04
Reconnaissance, Passive and Active
Run OSINT and network scanning, from open source information sources to SQL mapping.

05
PBED for Cyberspace Operations
Plan, Brief, Execute, and Debrief operations using the ME3C-(PC)2 planning model.

06
Attack Across Networks and Systems
Exploit web, wireless, and network vulnerabilities with Metasploit, XSS, SQLi, and password cracking.

07
Persistent, Integrated Operations
Maintain access with C2, rootkits, and tunneling, then cover tracks across logs and artifacts.

08
Network Protection
Detect and counter intrusions with traffic analysis, vulnerability scanning, and IDS or IPS.

Mapping cybersecurity courses to the DoD Cyber Workforce Framework (DCWF) ensures direct compliance with DoD 8140 requirements and transforms standard training into targeted, role-based skills development. This alignment shifts the focus from checking a box with generalized certifications to validating specific operational capabilities across the defense sector.

PREREQUISITE RECOMMENDED: ICWOD

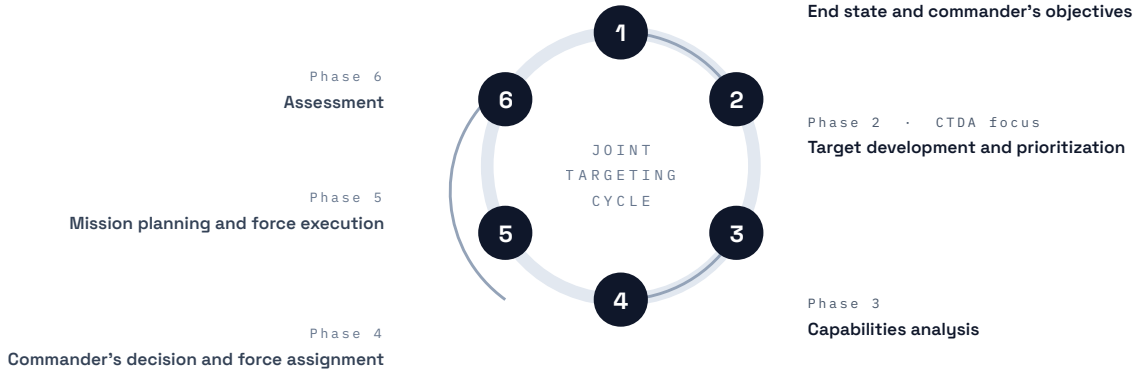
COURSE CODE CSFI-04 · CTDA

Cyber Target Development Analyst

A vital bridge between U.S. military operational level doctrine and tactical level implementation, built for the professionals responsible for developing and prioritizing targets in the cyber domain. It enriches existing joint and service doctrine; it does not replace it.

COURSE AT A GLANCE	
DURATION	3 days, 8 modules
DELIVERY	F2F, live, async
PREREQUISITE	ICWOD
SKILL LEVELS	Basic to Advanced
DOCTRINE	DoD and NATO

THE SIX PHASE JOINT TARGETING CYCLE · JP 3-60



WHAT YOU WILL MASTER

01
The Joint Targeting Process
Apply joint targeting principles and the six phase cycle to operations in and through cyberspace.

02
The Target Development Phase
Build targets to DoD standards at Basic, Intermediate, and Advanced levels.

03
Validation and Vetting
Validate targets against ethical and legal cyber recommendations and operational needs.

04
Targeting Intelligence
Run target intelligence research to complete every element of target development.

05
Weaponeering and Effects
Weigh capabilities, aimpoints, and collateral damage for precise, proportionate effects.

06
Dynamic Targeting
Apply F2T2EA standards to time sensitive, dynamic targets in the cyber domain.

THE FIVE TARGET TYPES

FACILITIES · INDIVIDUALS · VIRTUAL ENTITIES · EQUIPMENT · ORGANIZATIONS

CYBER THREAT INTELLIGENCE

SOC · ANALYSIS · STRATEGY

FIVE DAY CERTIFICATION · CCTI-A&S

Certified Cyber Threat Intelligence Analyst and Strategist

A five day intensive certification developed by the CSFI Cyber Threat Intelligence Division. It prepares professionals to operate across defense, intelligence, coalition, and enterprise environments, integrating doctrine, structured frameworks, hands-on tooling, and legal guardrails into one applied curriculum.

DIAMOND MODEL | MITRE ATT&CK | ODNI CTF | DISARM | MALTEGO | CYBER KILL CHAIN

COURSE AT A GLANCE	
DURATION	5 days, 40 hours
SCHEDULE	08:30 to 17:00 daily
CURRICULUM	9 units
FORMAT	Lecture, lab, exercise
CREDENTIAL	CCTI-A&S certification

WHAT YOU WILL BE ABLE TO DO

01

Structured Analytical Frameworks

Frame intrusion events and adversary activity into disciplined, defensible analytic judgments.

02

Intelligence Requirements

Manage requirements across IR, GIR, PIR, and RFI levels to drive the full intelligence cycle.

03

Hands-On Analytic Tooling

Analyze real adversary artifacts with Maltego, ATT&CK Navigator, JSON tooling, and OSINT.

04

ODNI Cyber Threat Framework

Map adversary behavior into timelines and layered, confidence rated judgments.

05

Influence and Information Operations

Analyze disinformation campaigns using the DISARM Red and Blue taxonomies.

06

Legal and Policy Guardrails

Navigate authorities, oversight, classification, and controlled dissemination.

Developed and delivered by the CSFI Cyber Threat Intelligence Division. Open to government, military, and qualified private sector participants.

CSFI · CYBER THREAT INTELLIGENCE DIVISION

Decision-quality cyber threat intelligence.

Tailored, evidence based intelligence that helps leaders, SOC teams, incident responders, and security programs understand threats, prioritize action, and defend decisions with confidence. Trusted products, without platform lock-in.

THE CTI DIVISION

PLATFORM-FREE · EVIDENCE BASED · FRAMEWORK DRIVEN

Platform-free reporting
Finished products you own, not another console to license.

Maturity assessments
Know where your CTI program stands and where to invest.

Framework enrichment
Reports mapped across the major intelligence frameworks.

Dissemination governance
Defensible release decisions, documented before you share.

CORE SERVICES · STRATEGIC

Strategic intelligence

What the threat means, who is behind it, and where to put the next dollar of defense. Executive RFI, sector and geography assessment, adversary intent.

CORE SERVICES · OPERATIONAL

Operational intelligence

Intelligence that moves at the speed of an incident. Campaign and vulnerability surge reporting, threat actor and infrastructure analysis.

CORE SERVICES · TECHNICAL

Tactical and technical

Where reporting becomes detection. IOC and TTP annexes, hunt packages, and framework mapping across ATT&CK, D3FEND, and STIX 2.1.

THE CSFI CTI INTERNSHIP

Answer the call. Defend forward.

U.S. citizen students join the CTI Division for guided cycles of real tradecraft: OSINT research, structured intelligence reporting, and threat actor profiling on live questions. Outstanding service can be recognized through the President's Volunteer Service Award program.

INTERNSHIP OPEN TO U.S. CITIZENS ONLY

- A CHINA
- B DPRK AND EAST ASIA
- C RUSSIA AND EURASIA
- D IRAN AND MENASWA
- E EMERGING THREATS
- F CYBER LAW AND POLICY
- G RANSOMWARE
- H CVES

8	3	12	U.S.
INTELLIGENCE SECTIONS	CYCLES EACH YEAR	WEEKS OF GUIDED WORK	CITIZENS-ONLY COHORT

COMBINED EVENTS

Host a combined event with CSFI.

CSFI brings together allied governments, embassies, cyber commands, and global industry for combined events: roundtables, panels, and planning exercises built around a realistic scenario. ***Small by design and senior by default.***

BRASILIA, BRAZIL — III FORO IBEROAMERICANO DE DEFENSA CIBERNETICA

6 FLAGSHIP EVENTS

7 NATIONS IN ONE EXERCISE

3 CONTINENTS REACHED

3 HOST EMBASSIES AND COMMANDS

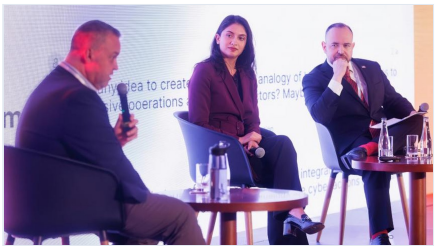
AI IN NATIONAL SECURITY

EMBASSY ROUNDTABLE

ON STAGE AT ITAPA

ALLIED DELEGATES

COMDCIBER, BRAZIL



CYBERSPACE OPERATIONS

The audience

Ambassadors, flag officers, agency leaders, and enterprise decision makers in one room.

The reach

A transatlantic and Americas footprint, hosted at embassies, commands, and institutions.

The format

Immersive, scenario driven roundtables and panels that spark candid, high signal dialogue.

The team

A trusted, non-profit team known across allied governments runs the event end to end.

SOME OF OUR CLIENTS

Trusted across defense, industry and intelligence.

GSA Multiple Award Schedule (MAS) Contract Holder

NSA · DOD · FBI · DISA · NATO · USAF · USMC · USCG · SAIC · LOCKHEED · MITRE · VISA

CSFI ADVISORY BOARD

Decades of intelligence and operational military command.

The CSFI Advisory Board brings together senior leaders from across the United States military, the intelligence community, federal government, academia, and industry. Their combined experience spans cyber operations, intelligence, defense, and national security at the highest levels of command, including retired general and flag officers.

MEET THE FULL BOARD

csfi.us/leadership.html

Biographies and appointments for every Advisory Director.

ADVISORY DIRECTOR

Mark Kelton

Former Deputy Director, National Clandestine Service for Counterintelligence, CIA

"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."

ADVISORY DIRECTOR

LtGen. (Ret.) John Toolan

United States Marine Corps

"The reputation of this organization [CSFI], particularly in the area of cyber and the information environment is stellar."

SPONSORS, PARTNERS AND ENDORSING INSTITUTIONS

CAPITOL Technology University · THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC · GEORGETOWN UNIVERSITY · G2OPS · Silobreaker · penlink · ICS · VALLEY FORGE MILITARY ACADEMY · CYBER BYTES FOUNDATION · skillsoft · CYBERSECURITY FINLAND · sectyne

START THE CONVERSATION

Train your people to the standard the mission actually demands.

WWW.CSFI.US

CONTACT@CSFI.US

Offices

Virginia Beach
2829 Guardian Lane,
Suite 150
Virginia Beach, VA 23452

Quantico office
1010 Corporate Drive
Stafford, VA 22554

Arlington office
901 N. Stuart St.
Suite 402
Arlington, VA 22203

Manassas office
Manassas
Virginia

CERTIFICATIONS

ICWOD · DCOE
CTDA · CCTI-A&S

TRAINING · EDUCATION · SERVICES · SUPPORTING THE AMERICAN WARFIGHTER IN CYBERSPACE