CERTIFICATION COURSE

CYBER TARGET DEVELOPMENT ANALYST

CTDA

The vital connection between U.S. military operational-level doctrine and tactical-level implementation for professionals responsible for targeting cyber assets.

DURATION	DELIVERY	PREREQUISITE
3 Days	Face-to-Face · Live Online · Async	ICWOD

WWW.CSFI.US

COURSE & CERTIFICATION

Cyber Target Development Analyst

TARGET DEVELOPMENT PHASE

Joint Targeting Cycle, integrated within the cyberspace operations framework.

Aligned to DoD Joint Targeting Development Standards and NATO joint/combined doctrine.

INTRODUCTION

The Cyber Target Development Analyst Certification Course is a vital connection between U.S. military operational-level doctrine and tactical-level implementation for professionals in cyberspace operations and cybersecurity, particularly those responsible for targeting cyber assets. This course will equip cyber professionals to understand and apply the joint targeting process. It focuses on the Target Development phase of the Joint Targeting Cycle, integrated within the cyberspace operations framework. While enriching existing Joint or Service doctrines, this course is not a substitute for them. The Cyber Security Forum Initiative (CSFI) offers training tailored for cyber personnel involved in joint targeting initiatives, ensuring high relevance and practicality. Additionally, the course provides well-articulated definitions that align with American and NATO joint/combined doctrine, sharing best practices from continuous military operations and exercises. Participants benefit from learning through examples and hands-on exercises.

OBJECTIVE

The course aims to provide procedures and techniques for target development for cyber analysts/operators, as outlined by the DoD Joint Targeting Development Standards. Equipped with target development procedures, reference materials, and the Joint Targeting Standards, students will develop targets at the Basic, Intermediate, and Advanced levels. This development aligns with Target Development standards for cyber operations and F2T2EA (Kill Chain) standards for dynamic targets. Students will become familiar with targeting intelligence and analysis techniques and standards for developing cyber operation targets using the DoD/NATO targeting doctrine.

COURSE DESCRIPTION

The Cyber Target Development Analyst (CTDA) Course introduces cyber analysts/operators to the essential skills required to develop various target types according to DoD target development standards for cyber operations. Throughout the course, analysts/operators will work on developing one of the five target types: facilities, individuals, virtual entities, equipment, and organizations. Classroom practical exercises will engage participants in target intelligence research and analysis, completing the elements required for target development. This includes Validating and Vetting targets in line with ethical cyber law recommendations and operational needs. These exercises enable the formation of concise and relevant statements for essential target development, encompassing aspects like target significance, description, functional characterization, expectation, critical elements, collateral damage considerations, intelligence gain/loss, target vulnerabilities, weaponeering, aimpoint selection and development, collateral damage estimate, and F2T2EA standards for dynamic targets.

We must defend against aggressive cyber threats from nations like China, Russia, Iran, and North Korea, ensuring our capabilities are synchronized around real-world warfighter needs.

Gen. Joshua M. Rudd

Commander, USCYBERCOM & Director, NSA

DOCTRINE ALIGNED WITH

United States Cyber Command
National Security Agency
Central Security Service

Foundations of Joint Targeting

MODULE 1

Introduction to DOD Joint Targeting Principles and Philosophies

- Overview of Targets and Targeting Responsibilities
- Target Description and Characteristics
- Categories of Targets
- Understanding Joint Targeting
- The purpose of Joint Targeting
- Principles of Targeting
- Targeting Prioritizations and Considerations
- Targeting and Joint Operation Planning
- The Joint Targeting Cycle
- Categories of Targeting
- Joint Force Targeting Duties and Responsibilities
- Joint Targeting Integration and Oversight
- Joint Force Staff Responsibilities
- Component Commander Responsibilities

MODULE 2

Introduction to the Joint Targeting Cycle and Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting

Overview of the Joint Targeting Cycle Phases:

- Phase 1—The End State and Commander's Objectives
- Phase 2—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—Targeting Assessment

- Relationship between Targeting and Effects

FIVE TARGET TYPES

Facilities · Individuals · Virtual Entities · Equipment · Organizations

DEVELOPMENT LEVELS

Basic · Intermediate · Advanced

Joint Targeting & Cyber Integration

MODULES 2, 4, 5, 6 · SIX-PHASE COMMAND WHEEL

PHASE 1
End State & Cdr's Objectives
INPUT
Center of Gravity Analysis

PHASE 2
Target Development & Prioritization
CORE
Cyber TLM Management

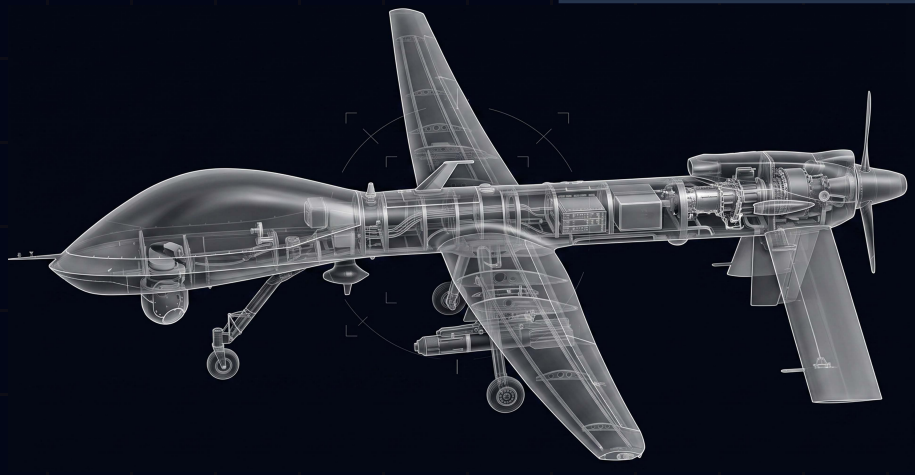
PHASE 3
Capabilities Analysis
OUTPUT
Cyber Weaponeering & CDE

PHASE 4
Cdr's Decision & Force Assignment
ASSIGN
Cyber Force Assignment

PHASE 5
Mission Planning & Force Execution
EXECUTE
F2T2EA Execution

PHASE 6
Targeting Assessment
ASSESS
Cyber Effects Assessment

CENTRAL HUB
Command Intent & Desired Effects



OUTER RING · SIX JOINT PHASES
INNER RING · CYBER INPUTS / OUTPUTS
FOCUS · PHASE 2 TARGET DEVELOPMENT

Cyber in the Joint Targeting Cycle

MODULE 3

Integrating Cyber Effects into the Joint Targeting Cycle

- USCYBERCOM's Role in Joint Targeting
- Integration of Cyberspace Operations in Joint Targeting according to DoD Targeting Doctrine
- Current Challenges and Improving Targeting Support to Cyberspace Operations
- Introduction to Cyber Target Development

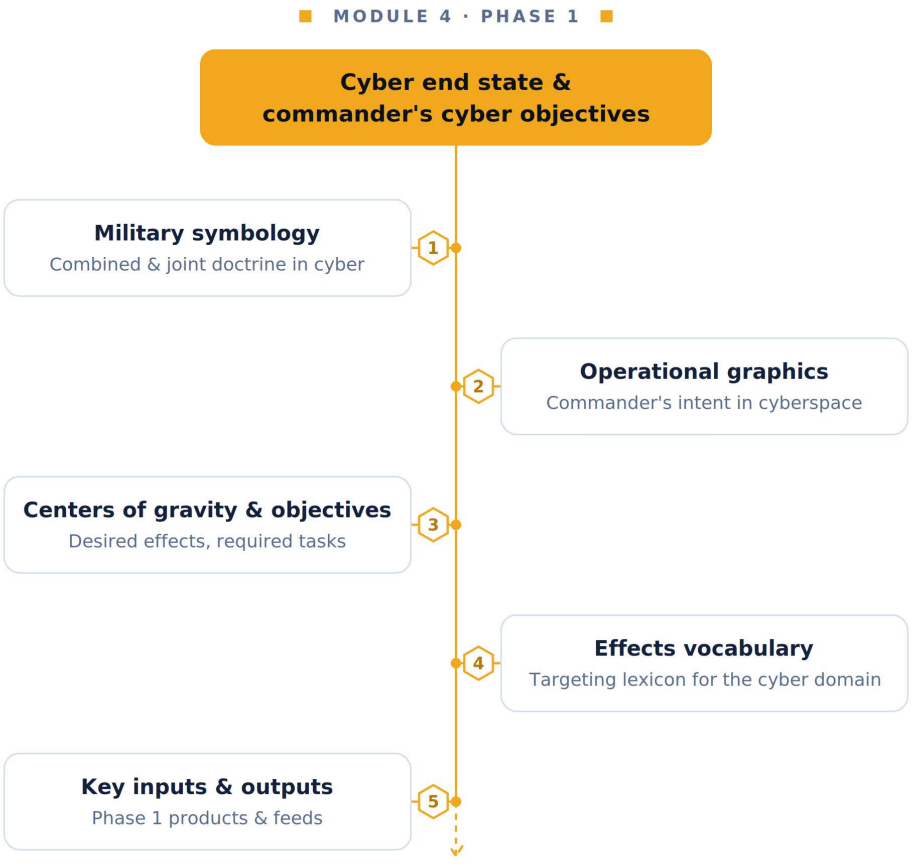
MODULE 4

Phase 1 of Cyber Target Development — Cyber End State and Commander/Leaders' Cyber Objectives

- Combined and Joint Military Symbology Doctrine in Cyberspace
- Operational Graphics and Joint Force Commanders' Intent in Cyberspace
- Understanding Centers of Gravity, Objectives, Desired Effects, and Required Tasks in Cyberspace
- Targeting Effects Vocabulary in the Cyber Domain
- Key Inputs and Outputs

USCYBERCOM · NSA · CSS

Synchronizing cyber capabilities around real-world warfighter needs.



Target Development Levels

MODULE 5 · ENTITY-LEVEL TARGET DEVELOPMENT

Targets are developed to three progressive levels of depth. Each level adds analytical rigor, compounding into a fully validated target profile.

DEPTH

	LEVEL 01 BASIC	LEVEL 02 INTERMEDIATE	LEVEL 03 ADVANCED
3	STEP 01 ☑ Cyber Target System Analysis	STEP 01 ☑ Critical Elements	STEP 01 ☑ Aimpoint Selection
2	STEP 02 ☑ Functional Characterization	STEP 02 ☑ Expectation Statement	STEP 02 ☑ Weaponeering
1	STEP 03 ☑ Significance Statement	STEP 03 ☑ Target Vulnerabilities	STEP 03 ☑ Collateral Damage Estimate

VALIDATED OUTPUT

Validated Target Profile

Each level compounds into a complete, vetted target folder ready for nomination.

- SIGNIFICANCE
- FUNCTIONAL
- CDE / IGL

Developing & Analyzing Cyber Targets

MODULE 5

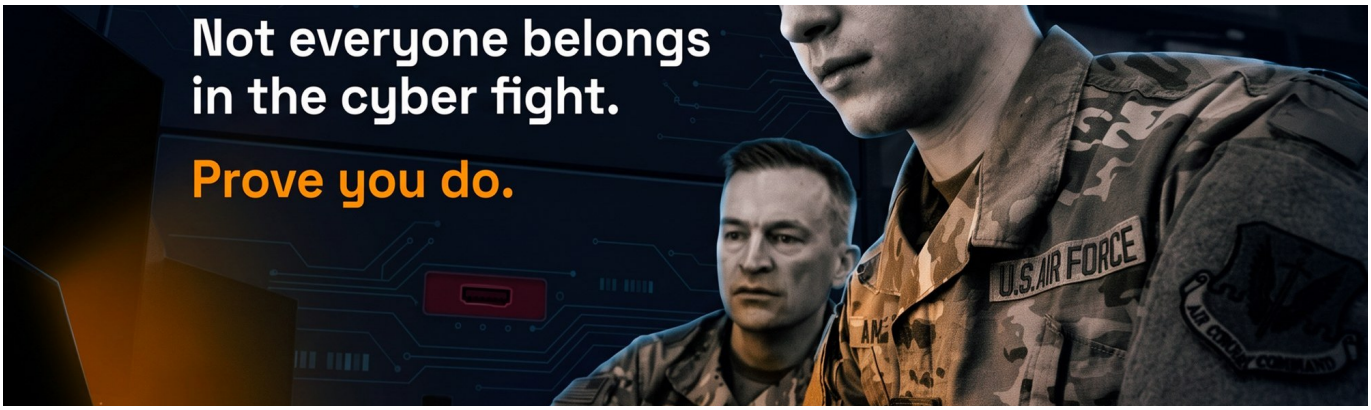
Phase 2 of Cyber Target Development — Cyber Target Development and Prioritization

- Cyber Target System Analysis
- Entity-Level Target Development (Basic, Intermediate, and Advanced)
- Electronic Folder Development
- Cyber Target List Management (TLM)
- Cyber Target Nomination for Prioritization, Synchronization, and Action

MODULE 6

Phase 3 of Cyber Target Development — Cyber Capabilities Analysis

- Target Cyber Vulnerability Analysis
- Cyber Capabilities Assignment
- Cyber Feasibility Assessment
- Cyber Effects Estimate
- Cyber Weaponeering
- Cyber Collateral Damage Estimation (CDE)



Cyber operators conduct target intelligence research and analysis in a live operations environment.

CYBER TARGET DEVELOPMENT · PROCESSING PIPELINE

PHASE 2 · MODULE 5
Cyber target development & prioritization

1. **Target system analysis** — Map the cyber target system
2. **Entity-level development** — Basic · intermediate · advanced
3. **Electronic folder development** — Build the electronic target folder
4. **Target list management** — TLM — tracking & upkeep
5. **Target nomination** — Prioritize · synchronize · action

PHASE 3 · MODULE 6
Cyber capabilities analysis

1. **Vulnerability analysis** — Find the target's weaknesses
2. **Capabilities assignment** — Match capability to target
3. **Feasibility assessment** — Can the effect be achieved?
4. **Effects estimate** — Predict the likely outcome
5. **Cyber weaponeering** — Tune & configure the cyber tool
6. **Collateral damage estimate** — CDE — gauge unintended impact

- Prioritized cyber targets from Phase 2 become the inputs to Phase 3 capabilities analysis.

Tactical Network Taxonomy

COURSE DESCRIPTION · FIVE TARGET TYPES

MASTER NODE

TARGET SYSTEM

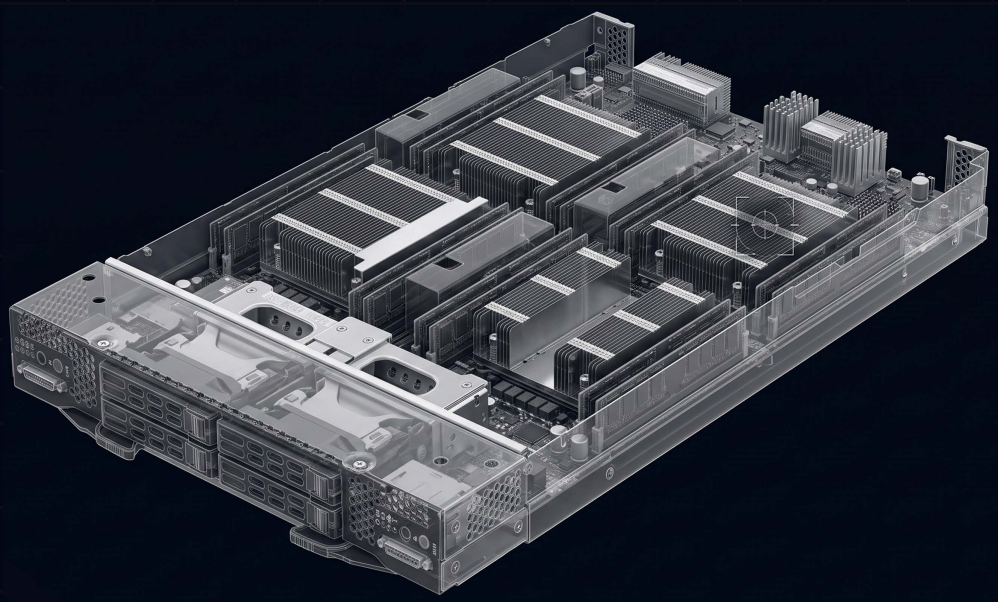
FACILITIES
- Production
- Command & Control
- Power & Utilities

INDIVIDUALS
- Key Personnel
- Operators
- Decision Makers

VIRTUAL ENTITIES
- IP Addresses
- Subnets
- Accounts

EQUIPMENT
- Routers
- Servers
- SCADA Hardware

ORGANIZATIONS
- Units
- Networks
- Support Elements



Analysts/operators develop one of the five target types, completing the elements required for target development: significance, description, functional characterization, critical elements, vulnerabilities, and F2T2EA standards for dynamic targets.

Legal & Ethical Cyber Targeting

MODULE 7 **Law of Armed Conflict and Rules of Engagement Considerations in Cyber Targeting**

- LOAC and International Law
- Rules of Engagement
- General Restrictions on Targeting
- Precautions in an Attack
- Separation of Military Activities
- Tallinn Manual: International Law Applicable to Cyber Operations

Legal Filtering Funnel

MODULE 7 · VALIDATION & VETTING SIEVE

TOP TIER · BROADEST

Tallinn Manual & International Law

LOAC · International Law · General Restrictions

MIDDLE TIER · INTERMEDIATE

Rules of Engagement (ROE)

Operational Constraints · Precautions

BOTTOM TIER · TIGHTEST

CDE & IGL Assessment

Collateral Damage Est. · Intel Gain/Loss

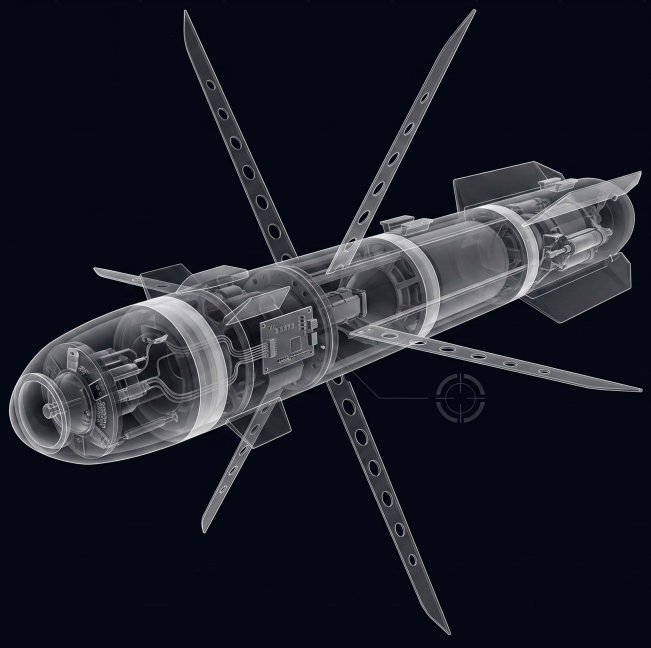
NEEDLE-EYE

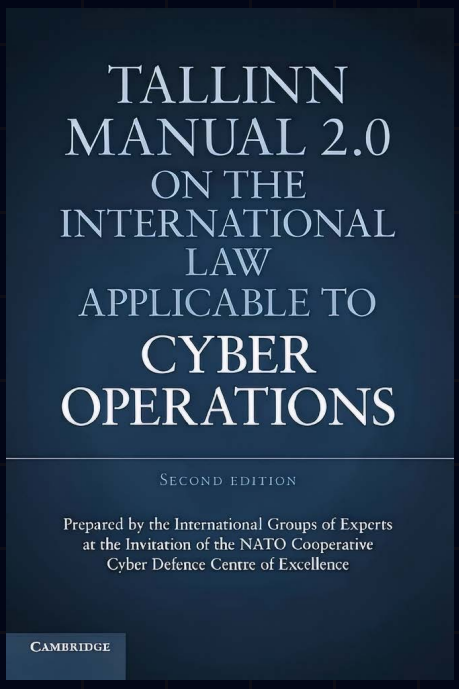
LEGALLY VETTED VECTOR

Approved Mission Path

REJECTED NON-VETTED

- Fails legal filter
- Fails legal filter
- Fails legal filter
- Fails legal filter





LEGALLY VETTED TARGET DATA

REJECTED · NON-VETTED

NEEDLE-EYE · APPROVED PATH

DAY 3 · REVIEW & CAPSTONE

Bringing It All Together

MODULE 8 **Review of Content**

- Comprehensive review of all modules and target development standards

CAPSTONE EXERCISE

Bringing It All Together to Successfully Develop a Cyber Target to DOD Joint Targeting Standards

COURSE LOGISTICS

DURATION
3 Days

PREREQUISITE
ICWOD

LOCATION
Face-to-Face · Live Online · Asynchronous

Aligns with F2T2EA (Kill Chain) standards for dynamic targets

Developed per DoD Joint Targeting Development Standards and DoD/NATO targeting doctrine, sharing best practices from continuous military operations and exercises.

DEFEND FORWARD

Prove you belong in the cyber fight.

Master the Target Development phase of the Joint Targeting Cycle. Develop cyber targets to DoD Joint Targeting Standards, validated and vetted in line with ethical cyber law.

Cyber Security Forum Initiative, Inc. (CSFI)

9401 Battle Street, Suite 202 Manassas, VA 20110, USA

WWW.CSFI.US

CAGE CODE 8L7W