CYBER TARGET DEVELOPMENT ANALYST (CTDA) COURSE AND CERTIFICATION

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.

Location:
Face-to-Face, Live Online, Asynchronous.

Duration:
3 Days.

Entry Prerequisites:
ICWOD

Cyber Target Development Analyst Course Outline

Day 1: Understanding DOD Joint Targeting Principles and Philosophies

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

Day 2:

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

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)

Day 3:

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

Module 8: Review of Content

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