CSFI · CYBER THREAT INTELLIGENCE DIVISION

5-DAY CERTIFICATION

CODE CCTI-A&S

Certified Cyber Threat Intelligence Analyst and Strategist

A five day intensive certification that prepares cyber threat intelligence professionals to operate across defense, intelligence, coalition, and enterprise environments, integrating doctrine, structured frameworks, hands on tooling, and legal guardrails into a single applied curriculum.

$4K
PER STUDENT

5
DAYS
40 HRS

9
UNITS
+ CAP

DEVELOPED BY THE CSFI CYBER THREAT INTELLIGENCE DIVISION

WWW.CSFI.US

CAPSTONE CERTIFICATION · INSTRUCTOR LED

COURSE OVERVIEW

Operationalize Cyber Threat Intelligence

The Certified Cyber Threat Intelligence Analyst and Strategist (CCTI-A&S) is a five day intensive certification developed by the Cyber Security Forum Initiative. It prepares CTI professionals to operate effectively across defense, intelligence, coalition, and enterprise environments by integrating foundational doctrine, structured analytical frameworks, hands on tooling proficiency, and legal guardrails into a single applied curriculum.

Nine units unfold across five days. Foundational frameworks come first, followed by requirements management, behavioral analysis, role and stakeholder mapping, technical analysis, and a concluding policy and synthesis. Every day pairs structured lecture and instructor led demonstration with hands on labs and team exercises with brief outs.

COURSE AT A GLANCE	
TUITION	$4,000 / person
DURATION	5 Days (40 Hours)
SCHEDULE	08:30 to 17:00
FORMAT	Lecture · Lab · Exercise
CURRICULUM	9 Units
CREDENTIAL	CCTI-A&S Cert.

REGISTER FOR CCTI-A&S

GOVERNMENT · MILITARY · QUALIFIED PRIVATE SECTOR

DEVELOPED BY

The CSFI Cyber Threat Intelligence Division

Instructor led, pairing lecture and demonstration with hands on labs and team exercises across forty instructional hours.

TRADECRAFT AT THE CORE

DIAMOND MODEL · CYBER KILL CHAIN · MITRE ATT&CK · PYRAMID OF PAIN · D3FEND · ODNI CTF · DISARM · MALTEGO · OSINT · JSON FOR CTI

COURSE OBJECTIVES

What You Will Be Able to Do

Upon successful completion, participants leave with six capabilities that translate directly into finished intelligence and confident decisions.

01

Structured Analytical Frameworks

Apply the Diamond Model and the Cyber Kill Chain to frame intrusion events and adversary activity into disciplined, defensible analytic judgments.

02

Intelligence Requirements, End to End

Manage requirements across IR, GIR, PIR, and RFI levels, capturing them from stakeholders and using them to drive the full intelligence cycle.

03

Hands On Analytic Tooling

Conduct analysis with Maltego, the MITRE ATT&CK Navigator, JSON tooling, and OSINT methods against real adversary artifacts and telemetry.

04

ODNI Cyber Threat Framework

Map adversary behavior and activity outputs to the ODNI Cyber Threat Framework, building layered, confidence rated judgments.

05

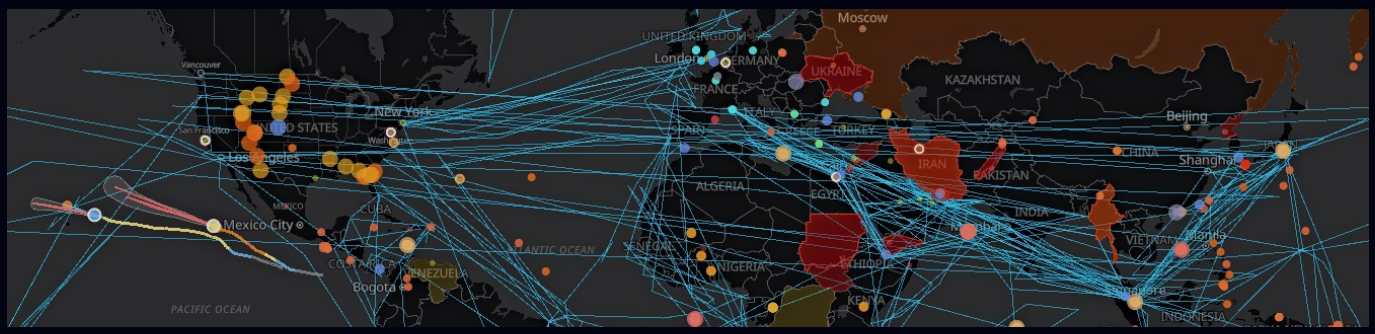
Influence and Information Operations

Analyze disinformation and influence campaigns using the DISARM Red and Blue taxonomies, from lookalike domains to forged content and amplification.

06

Legal and Policy Guardrails

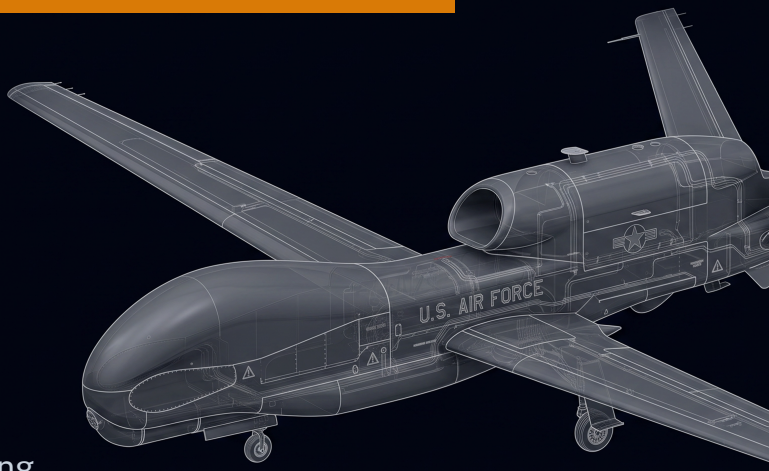
Navigate authorities, intelligence oversight, classification, and controlled dissemination so intelligence is shared lawfully and responsibly.



LIVE ADVERSARY ACTIVITY · GLOBAL THREAT LANDSCAPE

ANALYTIC DOCTRINE

No validated intelligence, no operation.



THAT IS THE STANDARD.

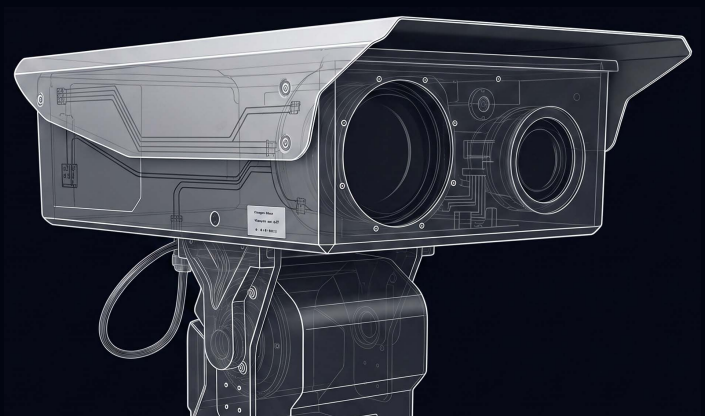
In military and national security operations, acting on unverified intelligence puts the mission, the force, and decision makers at risk. Cyber operations are no different. An unvalidated indicator is not intelligence; it is an assumption carrying operational consequences.

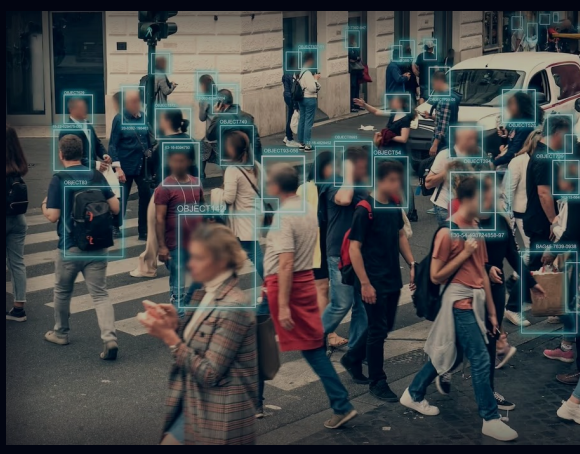
> **When confidence is low, the answer is not speed.**
> **It is discipline.**
>
> RE-COLLECT | CROSS-CUE | NARROW THE SCOPE | CHALLENGE THE ASSESSMENT
>
> Then make the decision.

Too many cyber responses have wasted manpower, disrupted operations, and damaged credibility because teams acted on indicators that later proved false. Those costs are real, and they compound quickly.

THE RULE IS CLEAR

Validate first. Execute second.





Nine Units Across Five Days

Foundational frameworks are introduced first, followed by requirements management, behavioral analysis, role and stakeholder mapping, technical analysis, and concluding policy and synthesis.

DAY	UNITS	FOCUS AREA
Day 1	Unit 1	**Foundations of Cyber Threat Intelligence** · the Diamond Model · applied analysis labs.
Day 2	Unit 2	**The Cyber Kill Chain** · phase by phase analyst use · reconnaissance and command and control labs.
Day 3	Units 3 & 4	**Intelligence Requirements** (IR, GIR, PIR, RFI) · Pyramid of Pain, MITRE ATT&CK, and D3FEND.
Day 4	Units 5, 9 & 6	**CTI roles and stakeholders** · DISARM framework · ODNI Cyber Threat Framework with the KONNI case.
Day 5	Units 7, 8 & Capstone	**JSON for CTI** · legal and policy guardrails · course synthesis and the certification capstone.

THE FIVE DAY FLOW · HOW THE WEEK BUILDS

DAY 1
Establish the Analytical Foundation

DAY 2
Apply the Adversary Lifecycle

DAY 3
Drive Analysis Through Requirements & Behavior

DAY 4
Map Roles, Taxonomies & Integrated Frameworks

DAY 5
Build Technical Proficiency, Governance & Synthesis

The Tradecraft You Will Apply

CCTI-A&S is built around the frameworks and tools that working CTI teams rely on every day, applied to real adversary cases throughout the week.

Diamond Model
Framing intrusion events across adversary, capability, infrastructure, and victim.

Cyber Kill Chain
The seven phase adversary lifecycle, from reconnaissance to actions on objectives.

Pyramid of Pain
Prioritizing indicators by the cost they impose on the adversary.

MITRE ATT&CK
Behavior to technique mapping and analysis in the ATT&CK Navigator.

D3FEND
Aligning detections and countermeasures to observed adversary techniques.

ODNI Cyber Threat Framework
A four layer model for structured, confidence rated analytic judgments.

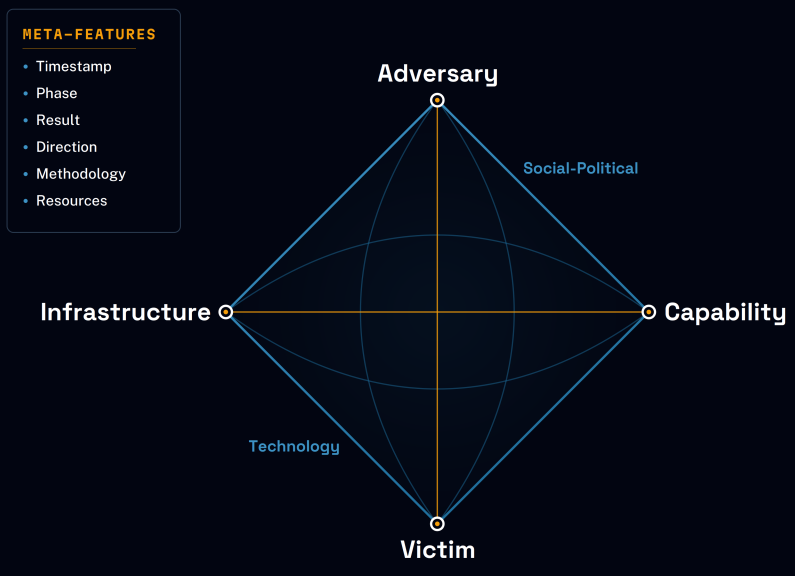
DISARM
Red and Blue taxonomies for influence and information operations analysis.

Maltego & OSINT
Link analysis and open source collection against real world artifacts.

JSON for CTI
Rapid reading and IOC extraction from structured telemetry and reporting.

Legal & Policy Guardrails
Authorities, oversight, markings, and controlled dissemination.

CORE ANALYTICAL MODEL · THE DIAMOND MODEL OF INTRUSION ANALYSIS



UNIT 01

Cyber Intelligence Foundations and the Diamond Model

28
TOPICS

Foundational intelligence concepts, collection, analysis, dissemination, the Diamond Model, and applied CTI laboratories.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- The Purpose of Intelligence
- Cyber Intelligence Challenge
- The Intelligence Cycle
- TCPED Process
- The Value of Cyber Intelligence
- Human Intent
- Active and Passive Collection Operations
- Cyber Intelligence Against Current and Emerging Threats
- Cyber Intelligence Dissemination
- Analytical Frameworks and Tooling
- Diamond Model for Intrusion Analysis
- Diamond Model axioms, vertices, events, meta-features
- Data, information, and intelligence relationships
- Intelligence requirements and Requests for Information
- Intelligence analysis and production
- **Cyber-enabled disinformation exercise: FAR and Hack4U**
- **Diamond Model attack-framing exercise**
- **Maltego Link-Analysis Lab: Syrian Electronic Army**
- **WhisperGate Malware Analysis Lab**
- **Iranian Malware and OSINT Analysis Lab**
- **Maltego, VirusTotal, and Cisco Talos indicator analysis**
- **EternalBlue and DoublePulsar attack-flow analysis**
- **PCAP and Wireshark analysis**
- **AI-assisted conversion of packet data into intelligence**
- **IOC extraction, ATT&CK mapping, reporting, defense**
- **EternalBlue Diamond Model analysis**
- **Group presentations**

DAY 2

UNIT 02

Cyber Kill Chain

30 TOPICS

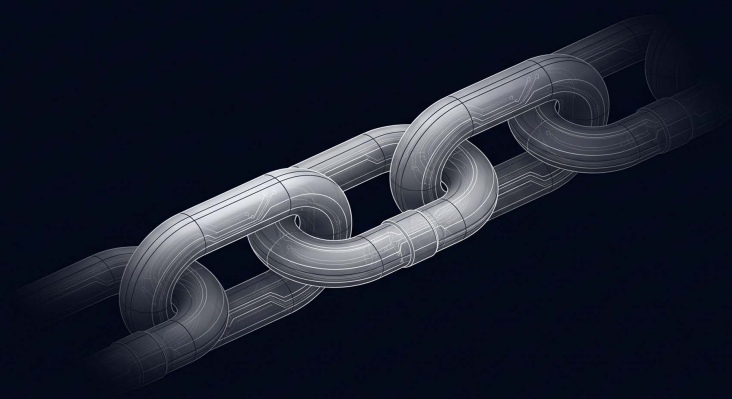
LOCKHEED MARTIN

Attack lifecycle analysis from reconnaissance through actions on objectives, supported by SolarWinds, C2, and critical-infrastructure scenarios.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Cyber Kill Chain overview
- Reconnaissance
- Active and passive reconnaissance
- **CSFI Reconnaissance Lab**
- Weaponization
- SolarWinds Orion/SUNBURST weaponization case study
- Trojanized software updates and backdoored DLLs
- Delivery
- Trusted vendor update channels
- Exploitation
- Delayed execution and sandbox or debugger checks
- Installation
- Malicious update installation and DLL placement
- Command and Control
- DNS beaconing
- Dynamic subdomains
- HTTPS command-and-control traffic
- Timing randomization and jitter
- **ICMP Tunneling and C2 Operations Lab**
- Actions on Objectives
- AD FS and SAML token abuse
- Cloud identity compromise
- Email, SharePoint, OneDrive, file-server access
- Data collection and staging
- Framing a cyberattack through the Kill Chain
- Nation-state industrial cyberattack scenario
- Stuxnet-like malware, zero-days, SCADA, PLC targeting
- Coordinated attacks on oil, gas, critical infrastructure
- Physical, business, emergency, and strategic effects
- **Defensive brainstorming and group presentation**



UNIT 03

Intelligence Requirements

19
TOPICS

Development, prioritization, capture, and operational use of IRs, GIRs, PIRs, and RFIs within the CTI intelligence cycle.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Intelligence Requirements framework: IR → GIR → PIR → RFI
- Intelligence Cycle in CTI
- Core definitions of IR, GIR, PIR, and RFI
- Intelligence Community doctrine alignment
- General Intelligence Requirements as strategic requirements
- Priority Intelligence Requirements as operational priorities
- Requests for Information as tactical requests
- End-to-end GIR → PIR → RFI example
- Strategic, operational, and tactical requirement differences
- Requirements scope, purpose, and duration
- U.S. Intelligence Community influence on CTI requirements
- Joint doctrine references
- Feedback loops and cross-functional collaboration
- SOC, legal, policy, and stakeholder inputs
- **Intelligence Stakeholder Interview Exercise**
- **Stakeholder Requirements Capture Lab**
- **Intelligence Planning Workbook**
- **Developing collection and delivery plans**
- **Requirements prioritization and briefing rationale**

REQUIREMENTS-DRIVEN ANALYSIS · THE CTI INTELLIGENCE CYCLE

DAY 3

UNIT 04

MITRE

Pyramid of Pain, MITRE ATT&CK, and D3FEND

40
TOPICS

Behavior-centric CTI mapping, ATT&CK Navigator analysis, defensive translation through D3FEND, and the LoJax UEFI rootkit case study.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Pyramid of Pain and its relationship to MITRE ATT&CK
- Hash values: MD5 and SHA-256
- IP addresses as infrastructure indicators
- Domain names and infrastructure durability
- Network and host artifacts
- Command-line, process, task, service, TLS, registry patterns
- Adversary tools, malware families, and frameworks
- Tactics, Techniques, and Procedures
- **Pyramid of Pain Mastery Exercise**
- MITRE ATT&CK tactics, techniques, sub-techniques
- Converting narrative reporting into behavior statements
- Repeatable CTI-to-ATT&CK mapping workflow
- Evidence extraction and behavior-statement development
- Confidence, procedure notes, and detection requirements
- MITRE ATT&CK Navigator
- Creating Enterprise ATT&CK layers
- Mapping, coloring, scoring, commenting, and linking
- Layer legends, labels, scoring models, quality control
- Exporting ATT&CK layers as JSON and PNG
- **Excel analysis of technique concentration and gaps**
- **ATT&CK Navigator layer-building mini-lab**
- **Operation Ghost / APT29 group capstone**
- D3FEND fundamentals
- Applying D3FEND to CTI
- D3FEND countermeasures and capability recommendations
- Rootkits and firmware-level persistence
- MITRE ATT&CK T1014: Rootkit
- D3FEND inferred relationships and defensive opportunities
- Process, kernel, memory, driver, firmware, boot analysis
- Detection hypotheses and evidence requirements
- LoJax UEFI rootkit attack flow
- APT28 and LoJax case study
- **CTI-report ingestion and D3FEND mapping lab**
- DoD tradecraft mapping
- Intelligence Preparation of the Cyberspace Environment
- Adversary Tradecraft Characterization
- Defensive Cyberspace Operations and DCO-IDM
- Tactical CTI report production
- Tactical CTI briefing for SOC and DCO audiences
- **CTI quality control and group presentation**

UNIT 05

Cyber Intelligence Roles and Stakeholders

18
TOPICS

Organizational CTI functions, stakeholder maturity, warning, awareness, and intelligence-driven support to security operations.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Cyber Intelligence Roles
- Collecting, analyzing, and delivering actionable intelligence
- Primary cyber-intelligence roles
- Predictive Threat Warning
- Threat Awareness
- Support to Security Operations
- Stakeholder roles
- Intelligence-literate stakeholders
- Educated stakeholders
- Intelligence practitioners
- Enterprise-risk decision support
- Strengthening security controls and operations
- Predictive Threat Warning in detail
- Strategic warning and organizational maturity
- Understanding current and emerging threat landscapes
- Intelligence-driven security operations
- Proactive versus reactive security operations
- **Day in the Life of a CTI Analyst**

INTELLIGENCE-DRIVEN SECURITY OPERATIONS · ROLES IN PRACTICE

Mark Kelton
CSFI Advisory Director
Former Deputy Director of the National Clandestine Service for Counterintelligence (DDNCS/CI) - 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." ***Mark Kelton***

UNIT 06

ODNI Cyber Threat Framework

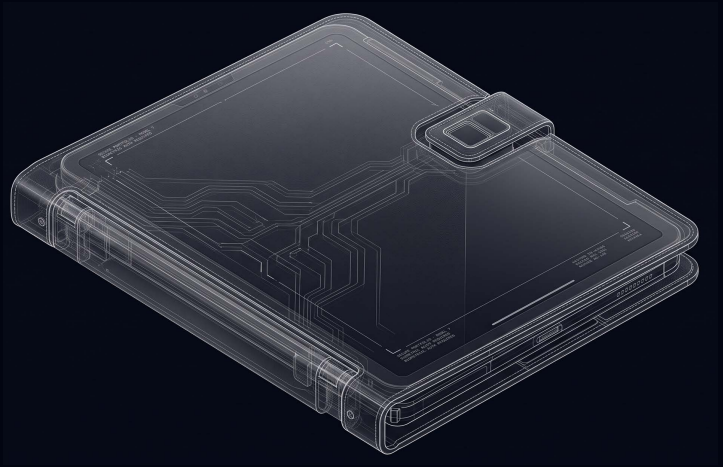
29
TOPICS

Application of the ODNI Cyber Threat Framework lifecycle and four-layer model to the North Korean KONNI intrusion.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- ODNI Cyber Threat Framework overview
- ODNI leadership and framework history
- ODNI CTF lifecycle
- Preparation
- Engagement
- Presence
- Effect and Consequence
- Applying the framework to a cyber incident
- Layer 1: Stages
- Layer 2: Objectives
- Layer 3: Actions
- Layer 4: Indicators
- ■ **ODNI CTF Excel template**
- North Korean KONNI case study
- Framing KONNI through the ODNI framework
- Attribution, targeting, lure themes, and intent
- Building an attack timeline
- Mapping timeline events to Layer 2 objectives
- Delivery of malicious capabilities
- Persistence and defense evasion
- Populating Layer 3 attacker actions
- PowerShell loading, staged payloads, scheduled tasks
- Populating Layer 4 indicators
- Assessing AI-assisted PowerShell tradecraft
- Privilege branching, anti-analysis, host fingerprinting
- Writing intelligence judgments with confidence levels
- ■ **Completing the ODNI worksheet**
- ■ **Producing an executive intelligence summary**
- KONNI attribution and intent assessment



UNIT 07

JSON for Cyber Threat Intelligence

31
TOPICS

Reading JSON as structured CTI, extracting indicators and context, and identifying KONNI persistence from endpoint telemetry.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Why JSON matters to CTI analysts
- JSON in EDR, SIEM, cloud logs, sandbox, APIs, MISP, STIX
- JSON basics
- Objects and named fields
- Arrays and lists
- Strings and values
- Nested data structures
- Key paths and dot notation
- Reading JSON as a structured CTI report
- Translating JSON structures into CTI meaning
- Preserving indicator value and context
- KONNI JSON case header
- Actor identification
- Delivery artifacts
- Persistence mechanisms
- File paths and staged payloads
- Command-and-control attributes
- IOC arrays and contextual fields
- Event timelines
- KONNI delivery chain
- PowerShell loader and backdoor
- Scheduled-task persistence
- In-memory execution
- C2 cookies, domains, IP addresses, and PHP endpoints
- ■ **Lab: Extracting IOCs from JSON**
- ■ **Structuring output as Type, Value, and Context**
- ■ **Grouping IOCs by attack stage**
- ■ **Lab: Identifying persistence from endpoint telemetry**
- Windows scheduled-task events
- Command-line and parent-process analysis
- Identifying stealth characteristics in telemetry

DAY 5

UNIT 08

CTI Legal and Policy Guardrails

37 TOPICS

Authorities, oversight, privacy, classification, markings, minimization, and controlled dissemination in DoD, IC, and coalition CTI environments.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- CTI legal and policy guardrails
- Why compliance guardrails matter to CTI operations
- Legal, privacy, and release requirements as planning inputs
- Title 10 military authorities
- Title 50 intelligence authorities
- Title 18 federal criminal-law authorities
- Collection, retention, use, and dissemination constraints
- CTI authority checks before sharing
- ORCON, FGI, NOFORN, REL TO, and partner caveats
- Intelligence Oversight
- U.S.-person information rules
- Least-intrusive means
- Reporting questionable intelligence activities
- U.S.-person minimization
- Masking and anonymization
- Retention, auditability, and documented justification
- Privacy-by-Design for CTI
- Practical minimization checklist
- Need-to-know, reduction, separation, marking, escalation
- Classification and portion marking
- Executive Order 13526
- Original and derivative classification
- CAPCO control markings
- Controlled Unclassified Information
- CUI versus TLP
- Dissemination decision points
- Tear lines
- Traffic Light Protocol 2.0
- Controlled sharing through STIX, TAXII, and MISP
- Distribution traceability and version control
- ICD 203 analytic standards
- Objectivity, transparency, relevance, and rigor
- ■ **Scenario Exercise: U.S.-person data in telemetry**
- ■ **Sharing restricted intelligence with NATO partners**
- ■ **Producing full-context and sanitized tear-line products**
- Sharing playbooks and after-action refinement
- ■ **Group presentation**

DISARM FOUNDATION

DAY 5

UNIT 09

DISARM and Influence Operations

42
TOPICS

Operationalizing influence intelligence through DISARM Red and Blue, narrative indicators, campaign mapping, OSINT, and short-form briefing.

INSTRUCTIONAL TOPICS & LABORATORIES

■ HANDS-ON LAB / EXERCISE

- Why DISARM matters to CTI
- Influence operations and disinformation as CTI problems
- Foreign Information Manipulation and Interference
- DISARM Red and DISARM Blue
- Shared taxonomy, evidence, and confidence
- Tagging behaviors
- Structuring campaigns
- Comparing influence actors
- Designing detections and mitigations
- DISARM and structured intelligence
- DISARM integration with STIX and TAXII
- DISARM and CTI threat convergence
- DISARM compared with MITRE ATT&CK
- DISARM Red adversary kill chain
- Planning, preparation, execution, and assessment
- DISARM Blue countermeasures
- Common language and cross-team coordination
- Faster triage and collection planning
- Coverage and gap analysis
- Repeatable response playbooks
- DISARM Blue operating model
- Phases, tactics, techniques, tasks, and counters
- Transitioning from IOCs to Indicators of Narrative
- Narrative indicators
- Actor infrastructure
- Tradecraft signals
- Cyber touchpoints
- Russia's Doppelganger web-forgery ecosystem
- Lookalike domains and imposter sites
- Forged articles and narrative laundering
- Coordinated amplification and persona activity
- Multi-language and multi-platform influence operations
- Campaign assessment through engagement signals
- **OSINT campaign-analysis lab**
- **Domain, page, posting-link, and historical evidence**
- **urlscan.io, Wayback Machine, WHOIS, InVID-WeVerify**
- **Mapping DISARM Red techniques and confidence**
- **Developing DISARM Blue countermeasures**
- **Producing a 60-second intelligence debrief**
- Evidence wording, attribution, mitigations, forecasting
- Tagging guidance and repeatable playbook development
- **Group presentation**

INTENDED AUDIENCE

Who Should Attend

The curriculum serves government, military, and qualified private sector practitioners alike. It is designed for those who need to integrate cyber threat intelligence into real decisions, products, and workflows.

- ✓ Mid career cyber threat intelligence analysts.
- ✓ All source intelligence professionals transitioning into cyber.
- ✓ Security operations personnel moving into intelligence roles.
- ✓ Joint and coalition cyber operators.
- ✓ Cyber strategists supporting defense and federal civilian organizations.

PREREQUISITES

A foundational understanding of cybersecurity concepts.

Basic familiarity with network defense.

An active operational or analytical need to integrate CTI into decisions, products, or workflows.

CERTIFICATION

A Credential Built on Tradecraft

The CCTI-A&S credential is awarded on successful completion of the five day program and its capstone. It reflects CSFI's commitment to producing intelligence professionals who apply rigorous analytic tradecraft, operate confidently within legal and policy guardrails, and translate technical observation into actionable intelligence judgments.

ENROLL

Reserve Your Seat

Tell us about yourself and your mission. A member of the CSFI team will follow up with scheduling, pricing, and enrollment details for CCTI-A&S.

ENROLL NOW · https://csfi.us/ccti.html