

# CHAPTER 20



## CRYPTOLOGIC TECHNICIAN (CT)

NAVPERS 18068-20K  
CH-63

Updated: July 2015

TABLE OF CONTENTS  
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

<b>SCOPE OF RATING</b>	CTN-3
<b>GENERAL INFORMATION</b>	CTN-4
<b>CRYPTOLOGIC CYBERSPACE ANALYST</b>	CTN-5
CYBER DEVELOPMENT AND EVALUATION	CTN-5
DEFENSIVE CYBER OPERATIONS (DCO)	CTN-5
FORENSIC ANALYSIS	CTN-5
MISSION COORDINATION	CTN-6
NETWORK ANALYSIS	CTN-6
OFFENSIVE CYBER OPERATIONS (OCO)	CTN-6
SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION	CTN-6
SYSTEMS ANALYSIS	CTN-7
TARGET DEVELOPMENT	CTN-7
VULNERABILITY ANALYSIS	CTN-7
<b>CYBERSPACE PLANNER</b>	CTN-8
CYBER PLANNING	CTN-8
MISSION COORDINATION	CTN-10
OFFENSIVE CYBER OPERATIONS (OCO)	CTN-10
SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION	CTN-10
TARGET DEVELOPMENT	CTN-10
VULNERABILITY ANALYSIS	CTN-10
<b>CRYPTOLOGIC CYBERSPACE OPERATOR</b>	CTN-11
CYBER DEVELOPMENT AND EVALUATION	CTN-11
DEFENSIVE CYBERSPACE OPERATIONS (DCO)	CTN-11
FORENSIC ANALYSIS	CTN-11
MISSION COORDINATION	CTN-12
NETWORK ANALYSIS	CTN-12
OFFENSIVE CYBER OPERATIONS (OCO)	CTN-12
SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION	CTN-12
SYSTEMS ANALYSIS	CTN-13
TARGET DEVELOPMENT	CTN-13
VULNERABILITY ANALYSIS	CTN-13

NAVY ENLISTED OCCUPATIONAL STANDARD  
FOR  
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)



SCOPE OF RATING

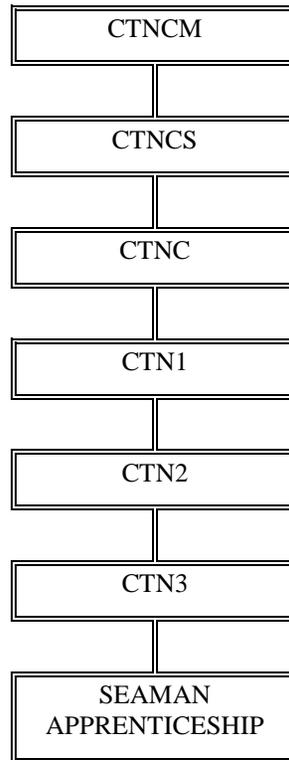
Cryptologic Technicians (Networks) (CTN) plan, develop, and execute offensive and defensive Cyberspace Operations; perform Cyber Defense, Digital Forensics, Network Exploitation, Research and Development, and Cyber Planning in support of national, fleet, and joint requirements.

---

This Occupational Standard is to be incorporated in Volume I, Part B, of the Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards (NAVPERS 18068F) as Chapter 20.

## GENERAL INFORMATION

### CAREER PATTERN



Normal path of advancement to Chief Warrant Officer and Limited Duty Officer categories can be found in OPNAVINST 1420.1.

For additional rating entry requirements, refer to MILPERSMAN 1306-618.

### SAFETY

**The observance of Operational Risk Management (ORM) and proper safety precautions in all areas is an integral part of each billet and the responsibility of every Sailor; therefore, it is a universal requirement for all ratings.**

**Job Title**

**Cryptologic Cyberspace Analyst**

**Job Code**

**003006**

**Job Family**

Computer and Mathematical

**NOC**

TBD

**Short Title (30 Characters)**

CRYPTOLOGIC CYBERSPACE ANALYST

**Short Title (14 Characters)**

CRYPTO CYB ANL

**Pay Plan**

Enlisted

**Career Field**

CTN

**Other Relationships and Rules**

Not applicable, based upon the NEC assigned to the job (if any).

**Job Description**

Cryptologic Cyberspace Analysts conduct analysis in support of offensive and defensive cyberspace operations to meet national, fleet, and joint requirements; and perform cyberspace target development and exploitation analysis, Indications and Warning (I&W), Attack Sensing and Warning (AS&W), forensic analysis, discovery, and counter-infiltration.

**DoD Relationship**

**Group Title**

Analysis

**DoD Code**

123200

**O\*NET Relationship**

**Occupation Title**

Computer Network Support Specialists

**SOC Code**

15-1152.00

**Job Family**

Computer and Mathematical

**Skills**

*Complex Problem Solving*

*Operations Analysis*

*Reading Comprehension*

*Active Learning*

*Judgment and Decision Making*

*Systems Analysis*

*Management of Personnel Resources*

*Mathematics*

*Systems Evaluation*

*Critical Thinking*

**Abilities**

*Inductive Reasoning*

*Selective Attention*

*Speech Clarity*

*Deductive Reasoning*

*Written Expression*

*Oral Expression*

*Originality*

*Written Comprehension*

*Mathematical Reasoning*

*Oral Comprehension*

**CYBER DEVELOPMENT AND EVALUATION**

**Paygrade**

E5

**Task Type**

NON-CORE

**Task Statements**

Configure virtualized development environments

E4

NON-CORE

Develop capabilities using basic level programming languages

E6

NON-CORE

Develop cyberspace operations tools, capabilities, and platforms

E6

NON-CORE

Interpret assembly code

E4

CORE

Interpret basic level source code

E5

NON-CORE

Interpret intermediate level source code

E7

NON-CORE

Maintain cyberspace operations tools, capabilities, and platforms

**DEFENSIVE CYBER OPERATIONS (DCO)**

**Paygrade**

E7

**Task Type**

CORE

**Task Statements**

Coordinate with Defensive Cyber Operations (DCO) partners and consumers

E4

CORE

Detect network vulnerabilities

E6

CORE

Evaluate information networks defensive posture of information networks

E5

CORE

Prevent unauthorized cyber operations

**FORENSIC ANALYSIS**

**Paygrade**

E7

**Task Type**

CORE

**Task Statements**

Coordinate forensic processes

E5

CORE

Document forensic processes and evidence collection

E6	NON-CORE	Perform advanced analysis
E5	CORE	Perform basic analysis
E4	CORE	Prepare target environments

#### **MISSION COORDINATION**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E7	NON-CORE	Coordinate cyberspace operations with partners
E6	CORE	Deconflict legal processes
E6	CORE	Deconflict network operations
E5	CORE	Identify potential threats posed by target networks
E7	CORE	Identify reportable intelligence
E6	CORE	Manage collection requirements
E7	CORE	Perform operational preparation of the environment in support of cyberspace operations
E7	CORE	Validate technical aspects of cyberspace operation products

#### **NETWORK ANALYSIS**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network vulnerabilities
E4	CORE	List network security architecture components
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis

#### **OFFENSIVE CYBER OPERATIONS (OCO)**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E5	CORE	Analyze raw data
E5	CORE	Analyze remote system environments
E5	CORE	Analyze remote targets for software pre-positioning
E4	CORE	Analyze software and hardware
E6	CORE	Assess technical impact of tools and techniques on a specific target
E5	NON-CORE	Develop offensive cyber Operations Plans (OPLAN)
E5	CORE	Maintain authorities based situational awareness
E5	NON-CORE	Maintain operational and technical situational awareness
E5	CORE	Provide technical solutions from all source data

#### **SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E4	CORE	Control access to restricted areas
E4	CORE	Destroy classified materials
E6	CORE	Document receipt of classified materials
E4	CORE	Implement Emergency Action Plans (EAP)
E4	CORE	Implement physical security measures
E4	CORE	Inventory classified materials
E7	CORE	Issue classified materials

E4	CORE	Maintain Sensitive Compartmented Information Facilities (SCIF) access control
E4	CORE	Safeguard classified materials
E4	CORE	Store classified materials
E5	CORE	Update classified materials

#### **SYSTEMS ANALYSIS**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E4	CORE	Analyze common system services
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze Operating System (OS) characteristics
E5	NON-CORE	Define basic structure and architecture of networks (e.g. wired, wireless, cellular)
E4	CORE	Define Operating System (OS) network roles for network devices
E4	CORE	Perform file system analysis (e.g. file structures, hierarchies, management, etc.)

#### **TARGET DEVELOPMENT**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E5	CORE	Analyze events for intelligence value
E4	CORE	Analyze metadata
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze remote target network functions
E5	CORE	Compile multiple source data
E4	CORE	Develop network map
E4	CORE	Develop target templates
E4	CORE	Gather target information
E4	NON-CORE	Provide cyber Concept of Operations (CONOP) input

#### **VULNERABILITY ANALYSIS**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E5	CORE	Analyze intrusion set activities
E5	CORE	Analyze network intrusion global threat activity data
E4	CORE	Analyze target network vulnerabilities
E6	CORE	Coordinate vulnerability scanning of target networks
E5	CORE	Report current/emerging cyber threats, intrusions, incidents, and events
E5	CORE	Report intrusion set activities

**Job Title**

**Cyberspace Planner**

**Job Code**

**003103**

**Job Family**

Management

**NOC**

TBD

**Short Title (30 Characters)**

CYBERSPACE PLANNER

**Short Title (14 Characters)**

CYBRSPACE PLNR

**Pay Plan**

Enlisted

**Career Field**

CTN

**Other Relationships and Rules**

Not applicable, based upon the NEC assigned to the job (if any).

**Job Description**

Cyberspace Planners perform in-depth targeting and cyber planning; conduct strategic and operational level planning across the full range of operations for integrated information and cyberspace operations; gather information; and develop detailed plans and orders in support of joint, fleet, and, national requirements.

**DoD Relationship**

**Group Title**

Analysis

**DoD Code**

123200

**O\*NET Relationship**

**Occupation Title**

Computer and Information  
Systems Managers

**SOC Code**

11-3021.00

**Job Family**

Management

**Skills**

*Judgment and Decision Making*

*Complex Problem Solving*

*Critical Thinking*

*Coordination*

*Reading Comprehension*

*Systems Evaluation*

*Operations Analysis*

*Systems Analysis*

*Active Learning*

*Writing*

**Abilities**

*Written Expression*

*Inductive Reasoning*

*Information Ordering*

*Written Comprehension*

*Mathematical Reasoning*

*Oral Comprehension*

*Oral Expression*

*Selective Attention*

*Speech Clarity*

*Deductive Reasoning*

**CYBER PLANNING**

**Paygrade**

E7

**Task Type**

CORE

**Task Statements**

Access event data to determine Commander's Critical Information Requirements (CCIR) criteria

E7

CORE

Analyze data (e.g. Battle Damage Assessment (BDA), measures of performance, measures of effectiveness)

E7

CORE

Assess strategic impact of tools and techniques on specific targets

E7

CORE

Conduct mission analysis

E7

CORE

Contact intelligence community partners to obtain cyber-related information

E7

NON-CORE

Coordinate cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners

E6

NON-CORE

Coordinate deployments to support cyberspace operations and exercises

E7

CORE

Counter enemy possible actions or reactions using Joint Intelligence Preparation of Operational Environment (JIPOE) information

E7

CORE

Determine best suited indicators to achieve cyberspace objectives

E7

CORE

Develop Concept of Operations (CONOP)

E7

CORE

Develop cyberspace operation support plans

E7

CORE

Develop cyberspace operations within Information Operations (IO) campaign plans

E7

CORE

Develop cyberspace-related plans (e.g. Operation Plan (OPLAN), Concept of Operations Plan (CONPLAN), Concept of Operations (CONOP), etc.)

E7

CORE

Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)

E7	CORE	Develop deliberate and/or crisis action plans
E7	CORE	Develop end state and commanders objectives
E7	CORE	Develop mission planning and force execution documents
E7	CORE	Develop Operational Plans (OPLAN) and Operational Orders (OPORD) at the strategic, operational, and tactical levels of warfare
E7	CORE	Develop target and prioritization
E7	CORE	Draft Cyber Effects Request Forms (CERF) in support of operational planning
E7	NON-CORE	Draft exercise schedule of events
E7	CORE	Evaluate planning cycle intelligence estimates
E7	CORE	Execute cyberspace-related plans (e.g. Operation Plan (OPLAN), Concept of Operations Plan (CONPLAN), Concept of Operations (CONOP), etc.)
E7	CORE	Gather synchronization of non-kinetic effects into the joint targeting cycle support data
E7	NON-CORE	Identify authorities and Standing Rules of Engagement (SROE) for cyberspace operations planning
E7	CORE	Identify cyber-related intelligence requirements
E7	CORE	Identify Intelligence gaps
E7	CORE	Implement course of action to address Commander's Critical Information Requirements (CCIR) event
E7	CORE	Implement cyberspace-related plans (e.g. Operation Plan (OPLAN), Concept of Operations Plan (CONPLAN), Concept of Operations (CONOP), etc.) and orders (e.g. Operational Orders (OPORD), Fragmentary Order (FRAGO), Warning Order (WARNORD), etc.)
E7	CORE	Incorporate Counter Espionage (CE), Cyber Counterintelligence (CI), Operation Security (OPSEC), and Communications Security (COMSEC) support plans
E7	CORE	Initiate cyberspace planning
E7	CORE	Integrate cyberspace planning efforts with other organizations and combatant commands
E7	CORE	Maintain deliberate and/or crisis action plans
E7	NON-CORE	Maintain situational awareness of cyber-related intelligence requirements
E7	CORE	Participate in long-range or strategic planning with other Department of Defense (DoD) and non-Department of Defense (DoD) cyberspace operations partners
E7	CORE	Perform Course of Action (COA) approvals
E7	CORE	Perform Course of Action (COA) comparison and wargaming
E7	CORE	Perform Course of Action (COA) development
E7	CORE	Perform cyberspace assessments
E6	NON-CORE	Prepare real world threat information scenarios
E7	CORE	Prioritize cyber-related intelligence requirements
E7	CORE	Provide operational support input (e.g. admin and log elements)
E7	CORE	Provide reporting (e.g. Battle Damage Assessment (BDA), measures of performance, and measures of effectiveness) to evaluate follow-on actions
E7	CORE	Recommend targets based on Signals Intelligence (SIGINT) reporting
E7	CORE	Respond to requests for deconfliction of cyberspace operations

E7	NON-CORE	Review capability analysis
E7	CORE	Review cyberspace-related Tactics, Techniques, and Procedures (TTP)

#### **MISSION COORDINATION**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E7	NON-CORE	Coordinate cyberspace operations with partners
E6	CORE	Deconflict legal processes
E6	CORE	Deconflict network operations
E5	CORE	Identify potential threats posed by target networks
E7	CORE	Identify reportable intelligence
E6	CORE	Manage collection requirements
E7	CORE	Perform operational preparation of the environment in support of cyberspace operations

#### **OFFENSIVE CYBER OPERATIONS (OCO)**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E6	CORE	Assess technical impact of tools and techniques on a specific target
E5	CORE	Conduct Computer Network Attack (CNA) operations
E5	CORE	Maintain authorities based situational awareness

#### **SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E4	CORE	Control access to restricted areas
E4	CORE	Destroy classified materials
E6	CORE	Document receipt of classified materials
E4	CORE	Implement Emergency Action Plans (EAP)
E4	CORE	Implement physical security measures
E4	CORE	Inventory classified materials
E7	CORE	Issue classified materials
E4	CORE	Maintain Sensitive Compartmented Information Facilities (SCIF) access control
E4	CORE	Safeguard classified materials
E4	CORE	Store classified materials
E5	CORE	Update classified materials

#### **TARGET DEVELOPMENT**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E5	CORE	Analyze events for intelligence value
E5	CORE	Compile multiple source data
E4	CORE	Gather target information
E4	NON-CORE	Provide cyber Concept of Operations (CONOP) input

#### **VULNERABILITY ANALYSIS**

<b><u>Paygrade</u></b>	<b><u>Task Type</u></b>	<b><u>Task Statements</u></b>
E5	CORE	Analyze network intrusion global threat activity data
E7	CORE	Assess target network vulnerabilities

**Job Title****Cryptologic Cyberspace Operator****Job Code****003303****Job Family**

Computer and Mathematical

**NOC**

TBD

**Short Title (30 Characters)**

CRYPTOLOGIC CYBERSPACE OPR

**Short Title (14 Characters)**

CRYPTO CYB OPR

**Pay Plan**

Enlisted

**Career Field**

CTN

**Other Relationships and Rules**

Not applicable, based upon the NEC assigned to the job (if any).

**Job Description**

Cryptologic Cyberspace Operators perform operations in support of offensive and defensive missions to meet national, fleet, and joint requirements; and perform exploitation and attack operations, software testing and evaluation, threat emulation, intelligence collection, and close access operations.

**DoD Relationship****Group Title**

Analysis

**DoD Code**

123200

**O\*NET Relationship****Occupation Title**

Computer Network Support Specialists

**SOC Code**

15-1152.00

**Job Family**

Computer and Mathematical

**Skills***Complex Problem Solving**Active Learning**Judgment and Decision Making**Operations Analysis**Reading Comprehension**Systems Analysis**Systems Evaluation**Critical Thinking**Management of Personnel Resources**Mathematics***Abilities***Inductive Reasoning**Deductive Reasoning**Selective Attention**Speech Clarity**Written Expression**Written Comprehension**Mathematical Reasoning**Oral Comprehension**Oral Expression**Originality***CYBER DEVELOPMENT AND EVALUATION****Paygrade****Task Type****Task Statements**

E4

NON-CORE

Develop capabilities using basic level programming languages

E5

NON-CORE

Develop capabilities using intermediate level programming languages

E6

NON-CORE

Evaluate cyberspace operations software tools, capabilities, and platforms

E6

NON-CORE

Interpret assembly code

E4

CORE

Interpret basic level source code

E5

NON-CORE

Interpret intermediate level source code

**DEFENSIVE CYBER OPERATIONS (DCO)****Paygrade****Task Type****Task Statements**

E4

CORE

Detect network vulnerabilities

E6

CORE

Evaluate information networks defensive posture of information networks

E5

CORE

Prevent unauthorized cyber operations

**FORENSIC ANALYSIS****Paygrade****Task Type****Task Statements**

E5

CORE

Perform basic analysis

E4

CORE

Prepare target environments

### MISSION COORDINATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Deconflict legal processes
E6	CORE	Deconflict network operations
E5	CORE	Identify potential threats posed by target networks
E7	CORE	Identify reportable intelligence
E7	CORE	Perform operational preparation of the environment in support of cyberspace operations
E7	CORE	Validate technical aspects of cyberspace operation products

### NETWORK ANALYSIS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network vulnerabilities
E4	CORE	List network security architecture components
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis

### OFFENSIVE CYBER OPERATIONS (OCO)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze raw data
E5	CORE	Analyze remote system environments
E5	CORE	Analyze remote targets for software pre-positioning
E4	CORE	Analyze software and hardware
E6	CORE	Assess technical impact of tools and techniques on a specific target
E6	NON-CORE	Conduct access operations
E6	NON-CORE	Conduct close access network operations
E5	CORE	Conduct Computer Network Attack (CNA) operations
E6	NON-CORE	Conduct Computer Network Exploitation (CNE) operations
E5	CORE	Maintain authorities based situational awareness
E5	CORE	Provide technical solutions from all source data
E6	NON-CORE	Survey collection and analysis of wireless data

### SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Control access to restricted areas
E4	CORE	Destroy classified materials
E6	CORE	Document receipt of classified materials
E4	CORE	Implement Emergency Action Plans (EAP)
E4	CORE	Implement physical security measures
E4	CORE	Inventory classified materials
E7	CORE	Issue classified materials
E4	CORE	Maintain Sensitive Compartmented Information Facilities (SCIF) access control

E4	CORE	Safeguard classified materials
E4	CORE	Store classified materials
E5	CORE	Update classified materials

#### SYSTEMS ANALYSIS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze common system services
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze Operating System (OS) characteristics
E5	NON-CORE	Define basic structure and architecture of networks (e.g. wired, wireless, cellular)
E4	CORE	Define Operating System (OS) network roles for network devices
E4	CORE	Perform file system analysis (e.g. file structures, hierarchies, management, etc.)

#### TARGET DEVELOPMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze events for intelligence value
E4	CORE	Analyze metadata
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze remote target network functions
E6	NON-CORE	Assess physical characteristics of the target environment
E5	CORE	Compile multiple source data
E6	NON-CORE	Construct virtualized network based on target data
E4	CORE	Develop network map
E4	CORE	Gather target information
E4	NON-CORE	Provide cyber Concept of Operations (CONOP) input

#### VULNERABILITY ANALYSIS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze target network vulnerabilities