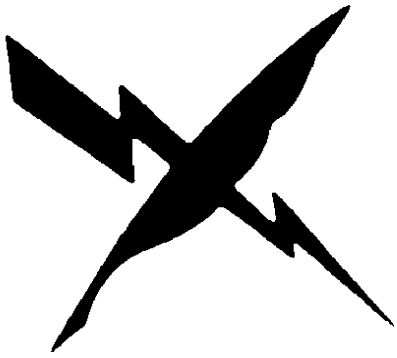
CHAPTER 20



CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

NAVPERS 18068F-20N
Change 95

Updated: July 2023

TABLE OF CONTENTS
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

TABLE OF CONTENTS (CONT'D)
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

NAVY ENLISTED OCCUPATIONAL STANDARD

FOR

CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

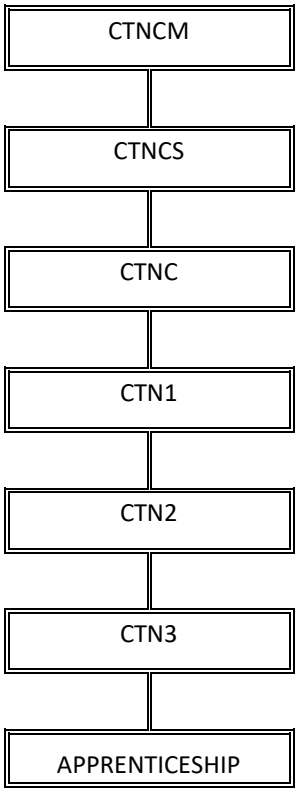
SCOPE OF RATING

Cryptologic Technicians (Networks) (CTN) employ strategic, operational and tactical capabilities to plan, develop, and execute offensive and defensive Cyberspace Operations; perform Hunt Operations, Threat Analysis, Digital Forensics, Network Exploitation, Research and Development, and Mission Planning; produce and execute cyberspace effects; leverage Signals Intelligence (SIGINT) and cryptologic functions to identify and report worldwide threats in support of Special Operations Forces (SOF), Fleet, National, and Joint requirements; and control and safeguard access to classified material and Information Systems (IS).

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 **Job Code**

Cyber Research And Development Specialist 002775

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	CYBER R&D SPECIALIST	CYB R&D SPEC

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyberspace Research and Development Specialists develop, test, and evaluate capabilities through reverse engineering, vulnerability research, and industry-standard development practices to enable offensive and defensive cyberspace operations.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Computer and Information Research Scientists	15-1111.00	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Complex Problem Solving	*Deductive Reasoning*
Judgment and Decision Making	*Written Expression*
Systems Analysis	*Selective Attention*
Systems Evaluation	*Information Ordering*
Coordination	*Problem Sensitivity*
Programming	*Originality*
Active Learning	*Written Comprehension*
Monitoring	*Speed of Closure*
Technology Design	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze Operating System (OS) characteristics
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat intelligence data
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Assess auditing and logging on target systems
E6	CORE	Assess event data to support Commander's Critical Information Requirements (CCIR) objectives
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Conduct dynamic binary analysis
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct memory analysis
E4	CORE	Detect network vulnerabilities
E4	CORE	Differentiate incidents and events from benign activities
E4	CORE	Evaluate containerization services
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E6	NON-CORE	Perform live memory analysis
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E5	CORE	Recommend targets based on all source reporting
E5	CORE	Validate target network vulnerabilities
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using compiled/assembled languages
E5	NON-CORE	Develop capabilities using scripting languages
E5	NON-CORE	Develop collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS))
E5	NON-CORE	Develop defensive and offensive cyberspace operations tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E7	NON-CORE	Establish guidelines for development cycles
E6	NON-CORE	Establish requirements for deployment of a capability
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Interpret assembly code
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform reverse engineering
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	NON-CORE	Utilize computer code to develop a software-based capability
E4	NON-CORE	Utilize open source code
E4	NON-CORE	Utilize secure coding techniques during development
E7	CORE	Validate requirements for capabilities
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COAs) analysis
E7	NON-CORE	Coordinate defensive or offensive cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E7	NON-CORE	Develop operational partnerships
E6	CORE	Evaluate Courses of Action (COAs) comparison
E4	CORE	Initiate Requests for Information (RFI)
E6	CORE	Maintain project management
E5	CORE	Maintain target situational awareness
E4	CORE	Navigate file systems
E7	CORE	Outline command and control activities
E5	NON-CORE	Perform asset validation
E4	CORE	Perform device exploitation
E4	CORE	Perform network enumeration and vulnerability analysis
E6	CORE	Perform operational risk assessment
E4	CORE	Perform wireless collection
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E4	CORE	Utilize a testing environment for capabilities
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Cyber Operations Planner 003103

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Management	TBD	CYBER OPERATIONS PLANNER	CYB OPS PLAN

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyberspace Operations Planners provide analytical support to the planning process derived from current capabilities, tool sets, and established accesses to meet Commander's intent and ensure objectives are achieved; participate in targeting selection, validation, and synchronization during the execution of cyber actions.

DoD Relationship

Group Title	*DoD Code*
Cyberspace Operations, General	127000

O*NET Relationship

Occupation Title	*SOC Code*	*Job Family*
Computer and Information Systems Managers	11-3021.00	Management

Skills	Abilities
Critical Thinking	*Written Expression*
Judgment and Decision Making	*Deductive Reasoning*
Complex Problem Solving	*Originality*
Coordination	*Inductive Reasoning*
Systems Analysis	*Problem Sensitivity*
Writing	*Information Ordering*
Systems Evaluation	*Oral Expression*
Active Learning	*Written Comprehension*
Monitoring	*Fluency of Ideas*
Quality Control Analysis	*Selective Attention*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	NON-CORE	Analyze intrusion set activities
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Identify access vectors for networks of interest
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E5	CORE	Recommend targets based on all source reporting

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E7	CORE	Validate requirements for capabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COAs) analysis
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E6	CORE	Conduct mission analysis
E6	NON-CORE	Conduct planning initiation
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	NON-CORE	Coordinate defensive or offensive cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Deconflict scheduled network operations
E6	NON-CORE	Determine capability requirements for development
E7	NON-CORE	Develop Commander's Critical Information Requirements (CCIR)
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop defensive tactical hunt plan
E5	NON-CORE	Develop offensive mission plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Develop operational plans, orders, and guidance
E7	CORE	Develop operational risk strategy
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate Courses of Action (COAs) comparison
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E6	CORE	Maintain project management
E5	CORE	Maintain target situational awareness
E6	CORE	Manage collection requirements
E7	NON-CORE	Manage unit priority target lists
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities
E4	CORE	Perform Defensive Cyberspace Operations (DCO)
E6	CORE	Perform exercise planning
E5	CORE	Perform mission analysis
E6	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	CORE	Perform wargaming
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	NON-CORE	Refine Priority Information Requirements (PIR)
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E7	CORE	Respond to operational and tactical deconfliction requests
E7	CORE	Validate collection requirements
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E6	NON-CORE	Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Cyber Defense Analyst 003104

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	CYBER DEFENSE ANALYST	CYB DEF ANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description
Cyberspace Defense Analysts collect, analyze and utilize host and/or network data in order to identify possible malicious activity and mitigate threats.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Information Security Analysts	15-1212.00	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Complex Problem Solving	*Deductive Reasoning*
Judgment and Decision Making	*Written Expression*
Systems Analysis	*Selective Attention*
Coordination	*Information Ordering*
Systems Evaluation	*Problem Sensitivity*
Operations Analysis	*Speed of Closure*
Monitoring	*Originality*
Active Learning	*Written Comprehension*
Operation and Control	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	NON-CORE	Analyze intrusion set activities
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network or system alerts from various sources
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat intelligence data
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E6	CORE	Assess event data to support Commander's Critical Information Requirements (CCIR) objectives
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	NON-CORE	Conduct host based forensics
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct memory analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop network map
E4	CORE	Differentiate incidents and events from benign activities
E4	NON-CORE	Document forensic processes and evidence collection
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E5	CORE	Validate target network vulnerabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E4	CORE	Develop heuristic or signature based detective and preventative measures
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	NON-CORE	Utilize open source code
E7	CORE	Validate requirements for capabilities
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E6	NON-CORE	Conduct incident response
E6	CORE	Conduct mission analysis
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E5	CORE	Deconflict scheduled network operations
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop defensive tactical hunt plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate Courses of Action (COAs) comparison
E5	CORE	Evaluate defense posture
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E5	CORE	Maintain situational awareness and functionality of operational infrastructure

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Maintain target situational awareness
E6	CORE	Manage collection requirements
E4	CORE	Navigate file systems
E7	CORE	Outline command and control activities
E5	NON-CORE	Perform asset validation
E4	NON-CORE	Perform Cyberspace Threat Hunting (CTH)
E4	CORE	Perform Defensive Cyberspace Operations (DCO)
E5	NON-CORE	Perform discovery and counter infiltration
E6	CORE	Perform exercise planning
E4	NON-CORE	Perform incident response
E5	CORE	Perform mission analysis
E4	CORE	Perform network enumeration and vulnerability analysis
E4	CORE	Perform network surveys
E6	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	NON-CORE	Perform untethered collections
E5	CORE	Perform wargaming
E4	CORE	Perform wireless collection
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Process data sets to tailor analytic efforts
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E4	CORE	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities
E7	NON-CORE	Refine Priority Information Requirements (PIR)
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Utilize a testing environment for capabilities
E7	CORE	Validate collection requirements
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	NON-CORE	Maintain evidence chain of custody
E5	NON-CORE	Manage forensic evidence
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Cyber Defense Forensics Analyst 003105

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	DEFENSE FORENSICS ANALYST	DEF FORE ANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyberspace Defense Forensics Analysts collect and analyze digital artifacts and investigate events to identify adversarial tactics, techniques, and procedures in order to inform threat mitigation efforts.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Digital Forensics Analysts	15-1299.06	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Complex Problem Solving	*Deductive Reasoning*
Judgment and Decision Making	*Selective Attention*
Systems Analysis	*Written Expression*
Systems Evaluation	*Information Ordering*
Active Learning	*Problem Sensitivity*
Coordination	*Speed of Closure*
Operations Analysis	*Originality*
Quality Control Analysis	*Written Comprehension*
Management of Material Resources	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	NON-CORE	Analyze intrusion set activities
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network or system alerts from various sources
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat intelligence data
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E6	CORE	Assess event data to support Commander's Critical Information Requirements (CCIR) objectives
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Conduct dynamic binary analysis
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	NON-CORE	Conduct host based forensics
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct mobile forensics
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Differentiate incidents and events from benign activities
E4	NON-CORE	Document forensic processes and evidence collection
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E6	NON-CORE	Manage forensic processes

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E6	NON-CORE	Perform live forensics
E6	NON-CORE	Perform live memory analysis
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E6	NON-CORE	Perform network device forensics
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform triage binary analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E5	CORE	Recommend targets based on all source reporting
E5	CORE	Validate target network vulnerabilities
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E4	CORE	Develop heuristic or signature based detective and preventative measures
E6	NON-CORE	Establish requirements for deployment of a capability
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Interpret assembly code
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions

CYBER DEVELOPMENT AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform reverse engineering
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	NON-CORE	Utilize computer code to develop a software-based capability
E4	NON-CORE	Utilize open source code
E7	CORE	Validate requirements for capabilities
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COAs) analysis
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E6	NON-CORE	Conduct incident response
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop defensive tactical hunt plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate Courses of Action (COAs) comparison
E7	CORE	Evaluate mission impact of tools and techniques on specific targets

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E5	CORE	Maintain situational awareness and functionality of operational infrastructure
E5	CORE	Maintain target situational awareness
E6	CORE	Manage collection requirements
E4	CORE	Navigate file systems
E7	CORE	Outline command and control activities
E5	NON-CORE	Perform asset validation
E4	NON-CORE	Perform Cyberspace Threat Hunting (CTH)
E4	CORE	Perform Defensive Cyberspace Operations (DCO)
E4	NON-CORE	Perform incident response
E5	CORE	Perform mission analysis
E4	CORE	Perform network enumeration and vulnerability analysis
E6	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Process data sets to tailor analytic efforts
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E4	CORE	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E4	CORE	Utilize a testing environment for capabilities
E7	CORE	Validate collection requirements
E7	CORE	Validate operational documents and reporting requirements

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	NON-CORE	Maintain evidence chain of custody
E5	NON-CORE	Manage forensic evidence
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Cyber Exploitation Analyst 003106

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	EXPLOITATION ANALYST	EXPLOIT ANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyberspace Exploitation Analysts identify and assess vulnerabilities in targeted networks to facilitate the collection of critical information; and execute tactics to establish and maintain accesses for current and future operations.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Digital Forensics	15-1299.06	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Judgment and Decision Making	*Written Expression*
Complex Problem Solving	*Deductive Reasoning*
Systems Analysis	*Selective Attention*
Systems Evaluation	*Problem Sensitivity*
Coordination	*Speed of Closure*
Monitoring	*Information Ordering*
Operations Analysis	*Originality*
Active Learning	*Written Comprehension*
Reading Comprehension	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	NON-CORE	Analyze intrusion set activities
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop network map
E4	CORE	Develop target templates
E4	CORE	Differentiate incidents and events from benign activities
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform forensic triage
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E5	NON-CORE	Perform target geospatial analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E5	CORE	Recommend targets based on all source reporting
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E6	CORE	Conduct mission analysis
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E5	CORE	Deconflict scheduled network operations
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop offensive mission plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Develop operational plans, orders, and guidance
E7	CORE	Develop operational risk strategy
E5	CORE	Evaluate collection requirements
E5	CORE	Evaluate defense posture
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E6	CORE	Maintain project management
E5	CORE	Maintain target situational awareness
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities
E4	CORE	Perform device exploitation
E5	CORE	Perform mission analysis
E4	CORE	Perform network enumeration and vulnerability analysis
E4	CORE	Perform network surveys
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E6	CORE	Perform operational and tactical deconfliction

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	NON-CORE	Perform untethered collections
E5	CORE	Perform wargaming
E4	CORE	Perform wireless collection
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Process data sets to tailor analytic efforts
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E5	NON-CORE	Provide time sensitive geolocation information
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E7	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Utilize a testing environment for capabilities
E5	NON-CORE	Utilize cyberspace capabilities to enable access to networks of interest
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Access Network Operator 003107

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	ACCESS NETWORK OPERATOR	ACCESS NET OP

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Access Network Operators perform local and close-access expeditionary cyberspace operations as assigned in support of Special Operations Forces (SOF), Fleet, National, and Joint mission-sets; and operationally leverages full-spectrum cyberspace capabilities from maritime, air, and ground domains.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Digital Forensicst	15-1299.06	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Judgment and Decision Making	*Deductive Reasoning*
Complex Problem Solving	*Written Expression*
Systems Analysis	*Information Ordering*
Systems Evaluation	*Selective Attention*
Coordination	*Originality*
Monitoring	*Problem Sensitivity*
Operation and Control	*Speed of Closure*
Reading Comprehension	*Written Comprehension*
Active Learning	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E6	CORE	Assess event data to support Commander's Critical Information Requirements (CCIR) objectives
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	NON-CORE	Conduct host based forensics
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct mobile forensics
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop network map
E4	CORE	Develop target templates
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E4	CORE	Perform initial target development
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform protocol analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E5	CORE	Recommend targets based on all source reporting
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using compiled/assembled languages
E5	NON-CORE	Develop capabilities using scripting languages
E5	NON-CORE	Develop collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS))
E5	NON-CORE	Develop defensive and offensive cyberspace operations tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E6	NON-CORE	Establish requirements for deployment of a capability
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform rigorous and periodic testing of a capability

CYBER DEVELOPMENT AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	NON-CORE	Utilize open source code
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E5	NON-CORE	Assess Maritime Wireless Pattern of Life (POL)
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E4	NON-CORE	Conduct access network operations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COAs) analysis
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E4	NON-CORE	Conduct initial access operations
E4	NON-CORE	Conduct interactive operations
E6	CORE	Conduct mission analysis
E5	NON-CORE	Conduct non-standard collection operations
E5	NON-CORE	Conduct Sensitive Site Exploitations (SSE) operations
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	NON-CORE	Coordinate defensive or offensive cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E5	CORE	Deconflict scheduled network operations
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	NON-CORE	Develop Commander's Critical Information Requirements (CCIR)
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop offensive mission plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Develop operational plans, orders, and guidance
E5	NON-CORE	Erect ground and airborne Signals Intelligence (SIGINT) collection equipment
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate Courses of Action (COAs) comparison
E5	CORE	Evaluate defense posture
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E5	CORE	Maintain situational awareness and functionality of operational infrastructure
E5	CORE	Maintain target situational awareness
E7	NON-CORE	Manage unit priority target lists
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E4	CORE	Perform device exploitation
E6	CORE	Perform exercise planning
E5	CORE	Perform mission analysis
E4	CORE	Perform network enumeration and vulnerability analysis
E4	CORE	Perform network surveys
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E6	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	NON-CORE	Perform tactical Airborne Precision Geolocation (APGL) operations/Unmanned Aerial Systems (UAS) payload operations
E5	NON-CORE	Perform tactical Precision Geolocation (PGL)
E5	NON-CORE	Perform untethered collections
E4	CORE	Perform wireless collection
E5	NON-CORE	Perform wireless source validation
E4	CORE	Prepare summary report of events

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E7	NON-CORE	Prioritize Signals Intelligence (SIGINT) collection efforts
E4	CORE	Process data sets to tailor analytic efforts
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E5	NON-CORE	Provide time sensitive geolocation information
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E7	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Utilize a testing environment for capabilities
E5	NON-CORE	Utilize cyberspace capabilities to enable access to networks of interest
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	NON-CORE	Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E7	NON-CORE	Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Interactive Operator 003108

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	INTERACTIVE OPERATOR	INTERACTIVE OP

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description
Interactive Operators perform computer network exploitation, capabilities testing and evaluation, data acquisition, network navigation and forensic analysis.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Digital Forensics	15-1299.06	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Systems Analysis	*Deductive Reasoning*
Complex Problem Solving	*Selective Attention*
Judgment and Decision Making	*Written Expression*
Systems Evaluation	*Information Ordering*
Coordination	*Problem Sensitivity*
Active Learning	*Originality*
Operations Analysis	*Speed of Closure*
Operation and Control	*Written Comprehension*
Monitoring	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze common system services
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	NON-CORE	Conduct memory analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Differentiate incidents and events from benign activities
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E6	NON-CORE	Perform live memory analysis
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E5	CORE	Validate target network vulnerabilities
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems
E6	NON-CORE	Establish requirements for deployment of a capability
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	NON-CORE	Utilize open source code
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E4	NON-CORE	Conduct initial access operations
E4	NON-CORE	Conduct interactive operations

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E5	CORE	Deconflict scheduled network operations
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Develop operational plans, orders, and guidance
E5	CORE	Evaluate collection requirements
E5	CORE	Evaluate defense posture
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E5	CORE	Maintain target situational awareness
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E4	CORE	Perform device exploitation
E4	CORE	Perform network enumeration and vulnerability analysis
E4	CORE	Perform network surveys
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	NON-CORE	Perform untethered collections
E5	CORE	Perform wargaming
E4	CORE	Perform wireless collection
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E5	NON-CORE	Provide time sensitive geolocation information
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E4	CORE	Utilize a testing environment for capabilities
E5	NON-CORE	Utilize cyberspace capabilities to enable access to networks of interest
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Digital Network Analyst 003109

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	DIGITAL NETWORK ANALYST	DIG NET ANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description
Digital Network Analysts perform cyberspace target development, discovery, and analysis in support of offensive cyberspace operations.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Digital Forensics	15-1299.06	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Systems Analysis	*Deductive Reasoning*
Complex Problem Solving	*Selective Attention*
Judgment and Decision Making	*Written Expression*
Systems Evaluation	*Speed of Closure*
Monitoring	*Information Ordering*
Active Learning	*Problem Sensitivity*
Coordination	*Written Comprehension*
Operations Analysis	*Originality*
Reading Comprehension	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	NON-CORE	Analyze intrusion set activities
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	NON-CORE	Analyze Signals of Interest (SOI)

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis, to include mobile
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E4	NON-CORE	Create target/collection requests
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop network map
E4	CORE	Develop target templates
E4	CORE	Differentiate incidents and events from benign activities
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E4	NON-CORE	Identify communication transmission infrastructure
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform initial target development

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	NON-CORE	Perform static binary analysis
E5	NON-CORE	Perform target geospatial analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform triage binary analysis
E4	CORE	Perform wireless analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E5	CORE	Recommend targets based on all source reporting
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E6	NON-CORE	Validate target/collection requests

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E4	CORE	Configure virtualized environments
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E4	NON-CORE	Utilize open source code

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E4	CORE	Detect metadata and data of targeting significance
E7	NON-CORE	Develop operational partnerships
E5	CORE	Evaluate collection requirements
E5	CORE	Evaluate defense posture
E4	CORE	Initiate Requests for Information (RFI)
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E6	CORE	Maintain project management
E5	CORE	Maintain target situational awareness
E6	CORE	Manage collection requirements
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities
E4	CORE	Perform network enumeration and vulnerability analysis
E6	CORE	Perform operational and tactical deconfliction
E4	CORE	Perform wireless collection
E5	NON-CORE	Perform wireless source validation
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E7	NON-CORE	Prioritize Signals Intelligence (SIGINT) collection efforts
E4	CORE	Process data sets to tailor analytic efforts
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E5	NON-CORE	Provide time sensitive geolocation information
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E4	CORE	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities
E4	CORE	Report current or emerging cyberspace threats, intrusions, incidents, and events
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)
E4	CORE	Utilize a testing environment for capabilities
E7	CORE	Validate collection requirements
E7	CORE	Validate operational documents and reporting requirements

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E6	NON-CORE	Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E7	NON-CORE	Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities

Job Title **Job Code**

Cyber Threat Emulation Operator 003110

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	CYBER THREAT EMULATION OPER	THREAT EMU OP

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTN	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyberspace Threat Emulation Operators (CTEOs) replicate adversarial tactics, techniques and procedures to perform aggressive threat assessments in support of Commander's training and operational requirements to inform internal defense measures.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Penetration Tester	15-1299.04	Computer and Mathematical

Skills	Abilities
Critical Thinking	*Inductive Reasoning*
Judgment and Decision Making	*Deductive Reasoning*
Systems Analysis	*Written Expression*
Complex Problem Solving	*Selective Attention*
Systems Evaluation	*Information Ordering*
Coordination	*Problem Sensitivity*
Operation and Control	*Originality*
Active Learning	*Speed of Closure*
Quality Control Analysis	*Written Comprehension*
Monitoring	*Fluency of Ideas*

CYBER ANALYSIS

Paygrade	Task Type	Task Statements
E5	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network and system artifacts to identify potential malicious activity (e.g., logs, malware, and system configuration files, etc.)
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	CORE	Analyze Operating System (OS) characteristics
E5	CORE	Analyze operational environments for key terrain in cyberspace
E5	NON-CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	NON-CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event and network logs

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat intelligence data
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Assess auditing and logging on target systems
E5	NON-CORE	Assess physical characteristics of the target environment
E4	CORE	Assess target network vulnerabilities
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Conduct endpoint analysis (clients and servers)
E5	CORE	Conduct independent in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct memory analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop network map
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E4	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E4	CORE	Evaluate virtualization services
E4	CORE	Formulate regular expression statements
E4	CORE	Identify access vectors for networks of interest
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E5	CORE	Identify Intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Interpret source code at a basic level
E4	CORE	Maintain awareness of advancements in hardware and software technologies and their potential implications (e.g., attend training or conferences, reading, etc.)
E4	CORE	Perform all source research
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E4	CORE	Perform initial target development
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform packet analysis
E4	CORE	Perform protocol analysis
E4	CORE	Perform timeline analysis

CYBER ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform wireless analysis
E4	NON-CORE	Provide target Positive Identification (PID)
E5	CORE	Recommend targets based on all source reporting
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E5	CORE	Validate target network vulnerabilities
E4	CORE	Verify target capabilities

CYBER DEVELOPMENT AND EVALUATION

Paygrade	Task Type	Task Statements
E6	NON-CORE	Collaborate with stakeholders for capabilities
E5	NON-CORE	Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E5	NON-CORE	Correct errors in software-based capabilities
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Develop capabilities using scripting languages
E5	NON-CORE	Develop defensive and offensive cyberspace operations tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E6	NON-CORE	Establish requirements for deployment of a capability
E4	CORE	Evaluate advancements in hardware and software technologies and their potential implications
E5	NON-CORE	Evaluate defensive or offensive cyberspace operations tools, capabilities, and platforms
E5	NON-CORE	Maintain defensive or offensive cyberspace operations tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	NON-CORE	Utilize open source code
E7	CORE	Validate requirements for capabilities
E6	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test (OT)

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support defensive or offensive cyberspace operations and exercises
E6	CORE	Analyze data (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and tactics, techniques, and procedures on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E5	CORE	Communicate with defensive or offensive cyberspace operations partners
E4	CORE	Communicate with intelligence analysts and targeting organizations
E4	NON-CORE	Conduct access network operations
E6	CORE	Conduct Courses of Action (COAs) analysis
E7	NON-CORE	Conduct cyberspace engagement in support of Commander's objectives
E4	NON-CORE	Conduct initial access operations
E4	NON-CORE	Conduct interactive operations
E6	CORE	Conduct mission analysis
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for offensive or defensive cyberspace operations planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate defensive or offensive cyberspace operations
E7	CORE	Coordinate with customers about operational tool and platform requirements
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E5	CORE	Deconflict scheduled network operations
E4	CORE	Detect metadata and data of targeting significance
E6	NON-CORE	Determine capability requirements for development
E6	CORE	Develop Courses of Action (COAs)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop offensive mission plan
E7	NON-CORE	Develop operational partnerships
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate Courses of Action (COAs) comparison
E5	CORE	Evaluate defense posture
E7	CORE	Evaluate mission impact of tools and techniques on specific targets
E4	CORE	Initiate Requests for Information (RFI)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Integrate cyberspace collections in intelligence gathering operations
E4	CORE	Maintain operational situational awareness
E6	CORE	Maintain project management
E5	CORE	Maintain situational awareness and functionality of operational infrastructure
E5	CORE	Maintain target situational awareness
E7	NON-CORE	Manage unit priority target lists
E4	CORE	Navigate file systems
E5	NON-CORE	Perform asset validation
E4	CORE	Perform Defensive Cyberspace Operations (DCO)
E4	CORE	Perform device exploitation
E6	CORE	Perform exercise planning
E4	NON-CORE	Perform incident response
E5	CORE	Perform mission analysis
E4	CORE	Perform network enumeration and vulnerability analysis
E4	CORE	Perform network surveys
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E4	NON-CORE	Perform offensive tactics in support of Defensive Cyberspace Operations (DCO)
E6	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE) in support of defensive or offensive cyberspace operations
E6	CORE	Perform operational risk assessment
E5	NON-CORE	Perform untethered collections
E5	CORE	Perform wargaming
E4	CORE	Perform wireless collection
E4	CORE	Prepare summary report of events
E5	CORE	Prepare technical aspects of organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E6	CORE	Prepare the operational environment
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commander's Critical Information Requirements (CCIRs), voice reports, etc.)
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E5	CORE	Report time sensitive information
E6	CORE	Respond to formal Requests for Information (RFI)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Utilize a testing environment for capabilities
E5	NON-CORE	Utilize cyberspace capabilities to enable access to networks of interest
E7	CORE	Validate collection requirements
E7	CORE	Validate operational documents and reporting requirements
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Control access to Sensitive Compartmented Information Facility (SCIF)
E6	CORE	Coordinate legal compliance reviews
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of Sensitive Compartmented Information (SCI) materials
E4	CORE	Implement Emergency Action Plan (EAP)
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials
E4	CORE	Verify operational authorities