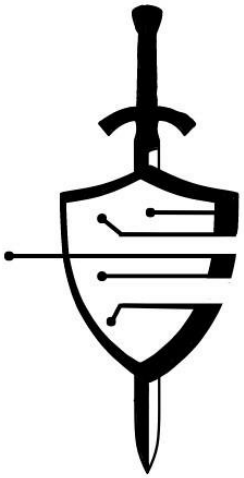
CHAPTER 20



CYBER WARFARE TECHNICIAN (CWT)

NAVPERS 18068F-20O
Change 101

Updated: January 2025

TABLE OF CONTENTS
CYBER WARFARE TECHNICIAN (CWT)

SCOPE OF RATING	**CWT-4**
GENERAL INFORMATION	**CWT-5**
CYBER RESEARCH AND DEVELOPMENT SPECIALIST	**CWT-6**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-6
CYBERSPACE ANALYSIS	CWT-7
CYBERSPACE OPERATIONS	CWT-8
SECURITY AND ADMINISTRATION	CWT-9
CYBER OPERATIONS PLANNER	**CWT-11**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-11
CYBERSPACE ANALYSIS	CWT-11
CYBERSPACE OPERATIONS	CWT-12
SECURITY AND ADMINISTRATION	CWT-14
CYBER DEFENSE ANALYST	**CWT-15**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-15
CYBERSPACE ANALYSIS	CWT-16
CYBERSPACE OPERATIONS	CWT-18
SECURITY AND ADMINISTRATION	CWT-21
CYBER EXPLOITATION ANALYST	**CWT-22**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-22
CYBERSPACE ANALYSIS	CWT-23
CYBERSPACE OPERATIONS	CWT-25
SECURITY AND ADMINISTRATION	CWT-27
EXPEDITIONARY CYBERSPACE OPERATOR	**CWT-28**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-28
CYBERSPACE ANALYSIS	CWT-29
CYBERSPACE OPERATIONS	CWT-31
SECURITY AND ADMINISTRATION	CWT-33
CYBERSPACE OPERATOR	**CWT-35**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-35
CYBERSPACE ANALYSIS	CWT-36
CYBERSPACE OPERATIONS	CWT-38
SECURITY AND ADMINISTRATION	CWT-39

TABLE OF CONTENTS (CONT'D)
CYBER WARFARE TECHNICIAN (CWT)

OFFENSIVE CYBERSPACE ANALYST	**CWT-40**
CYBER RESEARCH, DEVELOPMENT, AND EVALUATION	CWT-40
CYBERSPACE ANALYSIS	CWT-40
CYBERSPACE OPERATIONS	CWT-42
SECURITY AND ADMINISTRATION	CWT-44

NAVY ENLISTED OCCUPATIONAL STANDARD

FOR

CYBER WARFARE TECHNICIAN (CWT)

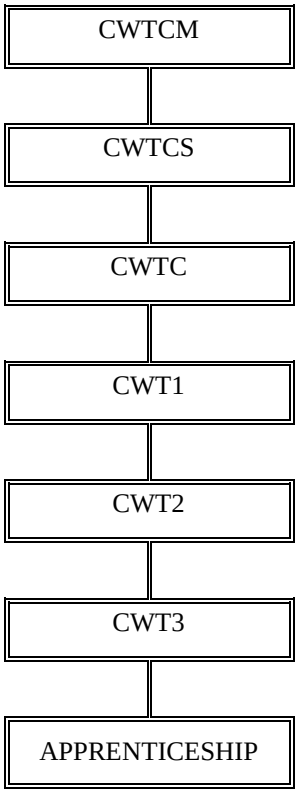
SCOPE OF RATING

Cyber Warfare Technician (CWT) employs strategic, operational, and tactical capabilities to plan, develop, and execute Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO); perform Cyberspace Threat Hunting (CTH) and analysis, digital forensics, network and host exploitation, Research and Development (R&D), and mission planning; execute cyberspace effects; leverage information and intelligence to identify, report, and respond to 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	CWT	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyber Research and Development Specialists develop, test, and evaluate capabilities through reverse engineering, vulnerability research, and industry-standard development practices to enable Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO).

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*
Systems Analysis	*Deductive Reasoning*
Judgment and Decision Making	*Selective Attention*
Complex Problem Solving	*Information Ordering*
Coordination	*Written Expression*
Systems Evaluation	*Problem Sensitivity*
Programming	*Written Comprehension*
Active Learning	*Fluency of Ideas*
Operation and Control	*Speed of Closure*
Mathematics	*Mathematical Reasoning*

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
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 software based capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E7	CORE	Coordinate with customers about operational tool and platform requirements
E4	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	Determine capability requirements for development
E4	NON-CORE	Develop capabilities using compiled/assembled languages
E4	NON-CORE	Develop capabilities using scripting languages
E4	NON-CORE	Develop collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS))
E4	NON-CORE	Develop Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E7	NON-CORE	Establish guidelines for development cycles
E5	NON-CORE	Establish requirements for deployment of a capability
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Formulate regular expression statements
E4	NON-CORE	Integrate foundational programming concepts for capability development
E4	NON-CORE	Interpret assembly code
E4	CORE	Interpret source code at a basic level
E5	NON-CORE	Maintain Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E6	NON-CORE	Perform advanced reverse engineering
E4	NON-CORE	Perform basic reverse engineering
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform intermediate reverse engineering
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E5	NON-CORE	Perform rigorous and periodic testing of a capability
E4	CORE	Utilize a testing environment for capabilities
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
E5	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test and Evaluation (OT&E)

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
E4	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	NON-CORE	Analyze memory capture
E4	CORE	Analyze metadata and data of targeting significance
E4	CORE	Analyze mobile operating system characteristics
E4	CORE	Analyze network security architecture components
E4	CORE	Analyze Operating System (OS) characteristics
E4	CORE	Analyze raw data

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze scanning activity
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	Analyze virtualization services
E5	NON-CORE	Assess physical characteristics of the target environment
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Conduct dynamic and static binary analysis
E5	CORE	Conduct in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis (e.g. mobile devices, hard drives, etc.)
E5	NON-CORE	Conduct memory analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Evaluate containerization services
E5	CORE	Evaluate virtualization services
E4	CORE	Identify applications and operating systems of a network device based on network traffic
E4	CORE	Identify communication transmission infrastructure
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Perform all source research
E4	CORE	Perform binary triage analysis
E4	NON-CORE	Perform dynamic and static binary analysis
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 vulnerability analysis
E4	CORE	Perform wireless analysis
E4	CORE	Process data sets to tailor analytic efforts
E5	CORE	Validate target network vulnerabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E4	CORE	Apply exploitation methodology

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and Tactics, Techniques, and Procedures (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E5	NON-CORE	Conduct memory capture
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Develop Courses of Action (COA)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E7	CORE	Develop operational partnerships
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E4	CORE	Initiate Requests for Information (RFI)
E6	CORE	Maintain project management
E4	CORE	Navigate file systems
E5	NON-CORE	Perform asset validation
E4	CORE	Perform device exploitation
E4	CORE	Perform scanning activity
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.)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
E5	CORE	Report cyberspace effects (e.g., Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.)
E6	CORE	Respond to formal Requests for Information (RFI)
E7	CORE	Validate target development recommendations
E4	CORE	Verify operational authorities

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)

SECURITY AND ADMINISTRATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Inventory Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials

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	CWT	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyber Operations Planners develop detailed plans and orders supporting Special Operations Forces (SOF), Fleet, National, and Joint requirements; develop and maintain deliberate and crisis action planning products; coordinate with cyberspace operators, analysts, and enablers to gain access and technical intelligence to meet planning objectives; and identify and levy requirements.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Computer and Information Systems Managers	11-3021.00	Management

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
E6	NON-CORE	Collaborate with stakeholders for capabilities
E7	CORE	Coordinate with customers about operational tool and platform requirements
E5	NON-CORE	Determine capability requirements for development
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E7	CORE	Validate requirements for capabilities

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze intrusion set activities
E5	CORE	Conduct in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E4	CORE	Define basic structure and architecture of networks
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	NON-CORE	Evaluate threats based upon vulnerabilities

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E6	CORE	Manage collection requirements
E4	CORE	Perform all source research
E5	CORE	Recommend targets based on all source reporting
E7	NON-CORE	Refine information requirements
E7	CORE	Validate collection requirements
E6	NON-CORE	Validate target and collection requests
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E5	CORE	Verify target capabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	NON-CORE	Advise Commander's Critical Information Requirements (CCIR)
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E4	CORE	Apply exploitation methodology
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and Tactics, Techniques, and Procedures (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E6	CORE	Conduct cyberspace engagement
E6	CORE	Conduct mission analysis
E6	NON-CORE	Conduct planning initiation
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E7	NON-CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Deconflict scheduled network operations
E5	CORE	Develop Courses of Action (COA)
E5	NON-CORE	Develop defensive analytic scheme of maneuver

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Develop defensive mission plan
E5	NON-CORE	Develop offensive mission plan
E7	CORE	Develop operational partnerships
E6	NON-CORE	Develop operational plans, orders, and guidance
E7	CORE	Develop operational risk strategy
E6	CORE	Evaluate Courses of Action (COA) comparison
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E5	CORE	Evaluate reporting requirements
E4	CORE	Initiate Requests for Information (RFI)
E6	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
E7	CORE	Outline command and control activities (e.g. supported and supporting relationships)
E6	NON-CORE	Perform exercise planning
E5	CORE	Perform mission rehearsal
E5	CORE	Perform operational and tactical deconfliction
E5	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.)
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), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
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)
E6	CORE	Respond to operational and tactical deconfliction requests
E7	CORE	Validate operational and tactical deconfliction requirements
E7	CORE	Validate operational documents
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities

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

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	CWT	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyber Defense Analysts perform in-depth analysis and forensics to identify Malicious Cyber Activity (MCA) and detect network anomalies; and discover, identify, assess, and mitigate intrusions vital to the protection of Fleet, National, and Joint Information Systems

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
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 software based capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E7	CORE	Coordinate with customers about operational tool and platform requirements
E4	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	Determine capability requirements for development
E4	NON-CORE	Develop capabilities using compiled/assembled languages
E4	NON-CORE	Develop capabilities using scripting languages
E4	NON-CORE	Develop collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS))
E4	NON-CORE	Develop Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools and platforms
E4	CORE	Develop heuristic or signature-based detective and preventative measures
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E7	NON-CORE	Establish guidelines for development cycles
E5	NON-CORE	Establish requirements for deployment of a capability
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Formulate regular expression statements
E4	NON-CORE	Interpret assembly code
E4	CORE	Interpret source code at a basic level
E5	NON-CORE	Maintain Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E5	NON-CORE	Perform Operational Evaluation (OE) of capabilities
E4	CORE	Utilize a testing environment for capabilities
E4	NON-CORE	Utilize open source code
E7	CORE	Validate requirements for capabilities

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
E4	CORE	Analyze cloud technology
E4	CORE	Analyze common system services
E4	CORE	Analyze identified malicious activity (e.g., determine weaknesses exploited, exploitation methods, effects on system and information, etc.)
E4	CORE	Analyze intrusion set activities
E4	NON-CORE	Analyze memory capture
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
E4	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze scanning activity
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event, and network logs

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Analyze threat intelligence data
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Analyze virtualization services
E5	CORE	Assess threat Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Conduct dynamic and static binary analysis
E5	NON-CORE	Conduct host based forensics
E5	NON-CORE	Conduct media analysis (e.g. mobile devices, hard drives, etc.)
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct mobile forensics
E5	CORE	Conduct tactical mission analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Detect network vulnerabilities
E5	NON-CORE	Determine data requirements
E4	CORE	Differentiate incidents and events from benign activities
E4	NON-CORE	Document forensic processes and evidence collection
E5	CORE	Evaluate collection requirements
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E5	CORE	Evaluate virtualization services
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
E6	CORE	Manage collection requirements
E7	NON-CORE	Manage unit priority target lists
E4	CORE	Perform all source research
E4	CORE	Perform binary triage analysis
E4	NON-CORE	Perform dynamic and static binary analysis
E4	CORE	Perform endpoint analysis (clients and servers)
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.)

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform network traffic analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform vulnerability analysis
E4	CORE	Perform wireless analysis
E4	CORE	Perform wireless source validation
E4	CORE	Process data sets to tailor analytic efforts
E7	NON-CORE	Refine information requirements
E7	CORE	Validate collection requirements
E6	NON-CORE	Validate Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Verify Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	NON-CORE	Advise Commander's Critical Information Requirements (CCIR)
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
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 (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E6	CORE	Conduct cyberspace engagement
E5	NON-CORE	Conduct incident response
E5	NON-CORE	Conduct interactive operations
E5	NON-CORE	Conduct memory capture
E6	CORE	Conduct mission analysis
E5	NON-CORE	Conduct non-standard collection operations
E6	NON-CORE	Conduct planning initiation
E5	NON-CORE	Conduct Sensitive Site Exploitations (SSE) operations
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	NON-CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Deconflict scheduled network operations
E5	CORE	Develop Courses of Action (COA)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop defensive analytic scheme of maneuver
E5	NON-CORE	Develop offensive mission plan
E7	CORE	Develop operational partnerships
E6	NON-CORE	Develop operational plans, orders, and guidance
E7	CORE	Develop operational risk strategy
E5	NON-CORE	Erect ground and airborne Signals Intelligence (SIGINT) collection equipment
E6	CORE	Evaluate Courses of Action (COA) comparison
E5	CORE	Evaluate defense posture
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E5	CORE	Evaluate reporting requirements
E5	NON-CORE	Harden physical and mobile networks
E4	CORE	Initiate Requests for Information (RFI)
E6	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
E6	NON-CORE	Manage data requirements
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities (e.g. supported and supporting relationships)
E5	NON-CORE	Perform asset validation
E4	NON-CORE	Perform Cyberspace Threat Hunting (CTH)
E4	CORE	Perform Defensive Cyberspace Operations (DCO)
E4	CORE	Perform device exploitation
E6	NON-CORE	Perform exercise planning
E4	CORE	Perform host enumeration
E4	NON-CORE	Perform incident response
E5	CORE	Perform mission rehearsal
E4	CORE	Perform network enumeration

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform network reconnaissance
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E4	NON-CORE	Perform offensive tactics in support of Defensive Cyberspace Operations (DCO)
E5	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE)
E5	CORE	Perform operational risk assessment
E4	CORE	Perform scanning activity
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
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.)
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), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E4	CORE	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities
E4	CORE	Recognize Mission Relevant Terrain in Cyberspace (MRT-C)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
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)
E6	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Support mission analysis
E5	NON-CORE	Utilize capabilities to enable access to networks of interest
E7	CORE	Validate operational and tactical deconfliction requirements
E7	CORE	Validate operational documents
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities
E5	CORE	Verify operational environments for key terrain in cyberspace

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	NON-CORE	Maintain evidence chain of custody
E4	NON-CORE	Maintain forensic evidence
E6	NON-CORE	Manage forensic processes
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Store Sensitive Compartmented Information (SCI) materials

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	CWT	NEC HXXX and 7XXX series and other NECs as assigned

Job Description

Cyber Exploitation Analysts identify and assess target device and network vulnerabilities for potential exploitation vectors to determine capability gaps, facilitate access, collection, network mapping, and cyber effects for current and future operations.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Computer Systems Analysts	15-1211.00	Computer and Mathematical

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
E6	NON-CORE	Collaborate with stakeholders for capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E7	CORE	Coordinate with customers about operational tool and platform requirements
E5	NON-CORE	Create algorithms to solve complex problems
E4	CORE	Create simple scripts (e.g., Python, PowerShell, UNIX Scripting, etc.)
E5	NON-CORE	Determine capability requirements for development
E4	NON-CORE	Develop capabilities using scripting languages
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Formulate regular expression statements
E4	CORE	Interpret source code at a basic level
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions
E4	CORE	Utilize a testing environment for capabilities
E7	CORE	Validate requirements for capabilities

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
E4	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	CORE	Analyze intrusion set activities
E4	NON-CORE	Analyze memory capture
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
E4	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze scanning activity
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event, and network logs
E4	CORE	Analyze target capabilities
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Analyze virtualization services
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 host based forensics
E5	CORE	Conduct in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis (e.g. mobile devices, hard drives, etc.)
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct mobile forensics
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E5	CORE	Conduct tactical mission analysis
E4	CORE	Define basic structure and architecture of networks

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop target templates
E4	CORE	Differentiate incidents and events from benign activities
E5	CORE	Evaluate collection requirements
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E5	CORE	Evaluate virtualization services
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	CORE	Identify communication transmission infrastructure
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Perform all source research
E4	CORE	Perform endpoint analysis (clients and servers)
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform initial target development
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E5	NON-CORE	Perform target geospatial analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform vulnerability analysis
E4	CORE	Perform wireless analysis
E4	CORE	Process data sets to tailor analytic efforts
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 Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E6	NON-CORE	Validate target and collection requests
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E5	CORE	Verify Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Verify target capabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
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 (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E6	CORE	Conduct cyberspace engagement
E6	NON-CORE	Conduct planning initiation
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E7	NON-CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Deconflict scheduled network operations
E5	CORE	Develop Courses of Action (COA)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop offensive mission plan
E7	CORE	Develop operational partnerships
E7	CORE	Develop operational risk strategy
E6	CORE	Evaluate Courses of Action (COA) comparison
E5	CORE	Evaluate defense posture
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E4	CORE	Initiate Requests for Information (RFI)
E6	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

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities (e.g. supported and supporting relationships)
E4	CORE	Perform device exploitation
E4	CORE	Perform host enumeration
E5	CORE	Perform mission rehearsal
E4	CORE	Perform network enumeration
E4	CORE	Perform network reconnaissance
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E4	NON-CORE	Perform offensive tactics in support of Defensive Cyberspace Operations (DCO)
E5	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE)
E5	CORE	Perform operational risk assessment
E4	CORE	Perform scanning activity
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.)
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	NON-CORE	Provide target Positive Identification (PID)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E4	CORE	Recognize Mission Relevant Terrain in Cyberspace (MRT-C)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
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)
E6	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Support mission analysis
E5	NON-CORE	Utilize capabilities to enable access to networks of interest
E7	CORE	Validate operational and tactical deconfliction requirements
E7	CORE	Validate operational documents
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities
E5	CORE	Verify operational environments for key terrain in cyberspace

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

Job Title **Job Code**

Expeditionary Cyberspace Operator 003107

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	EXP CYBERSPACE OPERATOR	EXP CYBR OPR

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

Job Description

Expeditionary Cyberspace Operators perform local and close-access expeditionary cyberspace operations as assigned in support of special operations forces, fleet national, and joint mission-sets. 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	Penetration Testers	15-1299.04	Computer and Mathematical

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
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 software based capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E7	CORE	Coordinate with customers about operational tool and platform requirements
E4	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	Determine capability requirements for development
E4	NON-CORE	Develop capabilities using compiled/assembled languages
E4	NON-CORE	Develop capabilities using scripting languages
E4	NON-CORE	Develop collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS))
E4	NON-CORE	Develop Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Ensure project continuity through documentation of design, testing, and implementation
E7	NON-CORE	Establish guidelines for development cycles
E5	NON-CORE	Establish requirements for deployment of a capability
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	CORE	Formulate regular expression statements
E4	NON-CORE	Integrate foundational programming concepts for capability development
E4	CORE	Interpret source code at a basic level
E5	NON-CORE	Maintain Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) 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	CORE	Utilize a testing environment for capabilities
E4	NON-CORE	Utilize open source code
E7	CORE	Validate requirements for capabilities
E5	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test and Evaluation (OT&E)

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
E4	CORE	Analyze common system services
E4	CORE	Analyze data to reconstruct and document target networks
E4	NON-CORE	Analyze memory capture
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
E4	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze scanning activity

CYBERSPACE 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 capabilities
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
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 host based forensics
E5	CORE	Conduct in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis (e.g. mobile devices, hard drives, etc.)
E5	NON-CORE	Conduct memory analysis
E5	NON-CORE	Conduct mobile forensics
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E5	CORE	Conduct tactical mission analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Detect network vulnerabilities
E5	NON-CORE	Determine data requirements
E4	CORE	Develop target templates
E5	CORE	Evaluate collection requirements
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	CORE	Evaluate scanning activity
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	CORE	Identify communication transmission infrastructure
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E7	NON-CORE	Manage unit priority target lists
E4	CORE	Perform all source research
E4	CORE	Perform binary triage analysis
E4	CORE	Perform endpoint analysis (clients and servers)
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform forensic triage
E4	CORE	Perform initial target development

CYBERSPACE 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
E5	NON-CORE	Perform target geospatial analysis
E4	CORE	Perform vulnerability analysis
E4	CORE	Perform wireless analysis
E4	CORE	Perform wireless source validation
E4	CORE	Process data sets to tailor analytic efforts
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 Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Validate target network vulnerabilities
E6	CORE	Validate target templates
E5	CORE	Verify Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Verify target capabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	NON-CORE	Advise Commander's Critical Information Requirements (CCIR)
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E4	CORE	Apply exploitation methodology
E5	NON-CORE	Assemble tactical infrastructure
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 (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E6	CORE	Conduct cyberspace engagement
E5	NON-CORE	Conduct initial access operations
E5	NON-CORE	Conduct interactive operations
E5	NON-CORE	Conduct memory capture
E6	CORE	Conduct mission analysis
E5	NON-CORE	Conduct non-standard collection operations
E6	NON-CORE	Conduct planning initiation

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	NON-CORE	Conduct Sensitive Site Exploitations (SSE) operations
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E7	NON-CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Deconflict scheduled network operations
E5	CORE	Develop Courses of Action (COA)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Develop offensive mission plan
E7	CORE	Develop operational partnerships
E6	NON-CORE	Develop operational plans, orders, and guidance
E7	CORE	Develop operational risk strategy
E5	NON-CORE	Erect ground and airborne Signals Intelligence (SIGINT) collection equipment
E6	CORE	Evaluate Courses of Action (COA) comparison
E5	CORE	Evaluate defense posture
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	NON-CORE	Harden physical and mobile networks
E4	CORE	Initiate Requests for Information (RFI)
E6	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
E6	NON-CORE	Manage data requirements
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E7	CORE	Outline command and control activities (e.g. supported and supporting relationships)
E4	CORE	Perform device exploitation
E6	NON-CORE	Perform exercise planning
E4	CORE	Perform host enumeration
E4	NON-CORE	Perform interactive operations
E5	CORE	Perform mission rehearsal
E4	CORE	Perform network enumeration
E4	CORE	Perform network reconnaissance

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E5	CORE	Perform operational and tactical deconfliction
E5	CORE	Perform Operational Preparation of the Environment (OPE)
E5	CORE	Perform operational risk assessment
E4	CORE	Perform scanning activity
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
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.)
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	NON-CORE	Provide target Positive Identification (PID)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E4	CORE	Recognize Mission Relevant Terrain in Cyberspace (MRT-C)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
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)
E6	CORE	Respond to operational and tactical deconfliction requests
E4	CORE	Support mission analysis
E5	NON-CORE	Utilize capabilities to enable access to networks of interest
E7	CORE	Validate operational and tactical deconfliction requirements
E7	CORE	Validate operational documents
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities
E5	CORE	Verify operational environments for key terrain in cyberspace

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

SECURITY AND ADMINISTRATION (CONT'D)

Paygrade	Task Type	Task Statements
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

Job Title **Job Code**

Cyberspace Operator 003108

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Computer and Mathematical	TBD	CYBERSPACE OPERATOR	CYBR OPR

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

Job Description

Cyberspace Operators employ a wide range of software applications for network navigation, tactical forensic analysis, surveillance and reconnaissance, and cyberspace effects in the execution of full-spectrum on-net, local, and close-access cyberspace operations.

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

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
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 software based capabilities
E4	CORE	Configure virtualized environments
E4	NON-CORE	Construct target environments for training, testing, and assessing
E7	CORE	Coordinate with customers about operational tool and platform requirements
E4	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	Determine capability requirements for development
E4	NON-CORE	Develop capabilities using compiled/assembled languages
E4	NON-CORE	Develop capabilities using scripting languages
E4	NON-CORE	Develop Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools and platforms
E5	NON-CORE	Develop new techniques for gaining and keeping access to target systems
E5	NON-CORE	Establish requirements for deployment of a capability
E5	NON-CORE	Evaluate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Formulate regular expression statements
E4	NON-CORE	Integrate foundational programming concepts for capability development
E4	CORE	Interpret source code at a basic level
E5	NON-CORE	Maintain Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) tools, capabilities, and platforms
E4	NON-CORE	Perform basic reverse engineering
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	CORE	Utilize a testing environment for capabilities
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
E5	NON-CORE	Validate tools, capabilities, and platforms during Developmental Test (DT) and Operational Test and Evaluation (OT&E)

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
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	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
E4	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze scanning activity
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	Analyze virtualization services

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
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 memory analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Detect network vulnerabilities
E4	CORE	Differentiate incidents and events from benign activities
E5	CORE	Evaluate collection requirements
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E5	CORE	Evaluate virtualization services
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	CORE	Identify communication transmission infrastructure
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E4	CORE	Perform all source research
E4	CORE	Perform binary triage analysis
E4	NON-CORE	Perform dynamic and static binary analysis
E4	CORE	Perform endpoint analysis (clients and servers)
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform vulnerability analysis
E4	CORE	Perform wireless analysis
E4	CORE	Reconnoiter remote targets (physical and virtual) for capability pre-positioning
E6	NON-CORE	Validate Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Validate target network vulnerabilities
E5	CORE	Verify Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E5	CORE	Verify target capabilities

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Apply exploitation methodology
E5	NON-CORE	Assemble tactical infrastructure
E4	CORE	Assess operational environment
E5	CORE	Assess technical impact of tools and Tactics, Techniques, and Procedures (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect forensic evidence
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct Courses of Action (COA) analysis
E6	CORE	Conduct cyberspace engagement
E5	NON-CORE	Conduct initial access operations
E5	NON-CORE	Conduct interactive operations
E5	NON-CORE	Conduct memory capture
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate cyberspace Operational Preparation of Environment (OPE)
E7	NON-CORE	Coordinate with external organizations to create and deploy tools
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E5	CORE	Deconflict scheduled network operations
E5	CORE	Develop Courses of Action (COA)
E5	CORE	Develop cyberspace-related Tactics, Techniques, and Procedures (TTP)
E7	CORE	Develop operational partnerships
E5	CORE	Evaluate defense posture
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E4	CORE	Initiate Requests for Information (RFI)
E6	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
E4	CORE	Navigate file systems
E5	NON-CORE	Nominate remote targets for software pre-positioning
E4	CORE	Perform device exploitation
E4	CORE	Perform host enumeration
E4	NON-CORE	Perform interactive operations
E5	CORE	Perform mission rehearsal
E4	CORE	Perform network enumeration

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Perform network reconnaissance
E4	CORE	Perform Offensive Cyberspace Operations (OCO)
E4	NON-CORE	Perform offensive tactics in support of Defensive Cyberspace Operations (DCO)
E5	CORE	Perform Operational Preparation of the Environment (OPE)
E5	CORE	Perform operational risk assessment
E4	CORE	Perform scanning activity
E5	NON-CORE	Perform untethered collections
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.)
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	NON-CORE	Provide target Positive Identification (PID)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E4	CORE	Recognize Mission Relevant Terrain in Cyberspace (MRT-C)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates
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
E5	NON-CORE	Utilize capabilities to enable access to networks of interest
E7	CORE	Validate operational documents
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities
E5	CORE	Verify operational environments for key terrain in cyberspace

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

Job Title **Job Code**

Offensive Cyberspace Analyst 003109

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Protective Service	TBD	OFFENSIVE CYBERSPACE ANALYST	OFF CYB ANLYST

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

Job Description

Offensive Cyberspace Analysts analyze metadata and content information to determine intelligence value, and reconstruct/document target networks; employ geospatial analysis techniques, maintain operational continuity, ensure continued collection, provide indications and warning, identify users, and all activities of associated targets; analyze target implementation of communication technologies and digital network systems by identifying vulnerabilities and potential exploitation vectors, suggest strategies and methods for target network, host system, and software and hardware exploitation.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Cyberspace Operations, General	127000	Intelligence Analysts	33-3021.06	Protective Service

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

CYBER RESEARCH, DEVELOPMENT, AND EVALUATION

Paygrade	Task Type	Task Statements
E6	CORE	Collaborate with Intelligence Community (IC) to obtain targeting or emerging technologies information
E7	CORE	Coordinate with customers about operational tool and platform requirements
E4	CORE	Formulate regular expression statements
E4	CORE	Interpret source code at a basic level
E4	CORE	Perform Boolean logic
E4	CORE	Perform discrete math functions

CYBERSPACE ANALYSIS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze audit and log files on Information Systems
E4	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	CORE	Analyze intrusion set activities
E4	NON-CORE	Analyze memory capture
E4	CORE	Analyze metadata and data of targeting significance

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task Statements
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
E4	CORE	Analyze operational environments for key terrain in cyberspace
E4	CORE	Analyze Operational Technology (OT) (e.g., Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), etc.)
E4	CORE	Analyze raw data
E4	CORE	Analyze remote system environments
E4	CORE	Analyze remote target network composition
E4	CORE	Analyze scanning activity
E4	CORE	Analyze software and hardware
E4	CORE	Analyze system, event, and network logs
E4	CORE	Analyze target capabilities
E4	CORE	Analyze target implementation of technologies and digital network systems
E4	CORE	Analyze threat Tactics, Techniques, and Procedures (TTP)
E4	CORE	Analyze virtualization services
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	CORE	Conduct in-depth target and technical analysis, to include target-specific information (e.g., cultural, organizational, political, etc.)
E5	NON-CORE	Conduct media analysis (e.g. mobile devices, hard drives, etc.)
E5	NON-CORE	Conduct Pattern of Life (POL) analysis
E5	CORE	Conduct tactical mission analysis
E4	CORE	Define basic structure and architecture of networks
E4	CORE	Detect metadata and data of targeting significance
E4	CORE	Detect network vulnerabilities
E4	CORE	Develop target templates
E4	CORE	Differentiate incidents and events from benign activities
E5	CORE	Evaluate collection requirements
E4	CORE	Evaluate containerization services
E6	CORE	Evaluate cyberspace-related Tactics, Techniques, and Procedures (TTP)
E5	CORE	Evaluate remote system environments
E5	CORE	Evaluate scanning activity
E5	NON-CORE	Evaluate threats based upon vulnerabilities
E5	CORE	Evaluate virtualization services

CYBERSPACE ANALYSIS (CONT'D)

Paygrade	Task Type	Task 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	CORE	Identify communication transmission infrastructure
E5	CORE	Identify intelligence gaps
E4	CORE	Identify technical solutions from all source data
E6	CORE	Manage collection requirements
E7	NON-CORE	Manage unit priority target lists
E4	CORE	Perform all source research
E4	CORE	Perform endpoint analysis (clients and servers)
E4	CORE	Perform file signature analysis
E4	CORE	Perform file system analysis
E4	CORE	Perform initial target development
E4	CORE	Perform mid-point analysis (e.g., routers, firewalls, switches, etc.)
E4	CORE	Perform network traffic analysis
E5	NON-CORE	Perform target geospatial analysis
E4	CORE	Perform timeline analysis
E4	CORE	Perform wireless analysis
E4	CORE	Perform wireless source validation
E4	CORE	Process data sets to tailor analytic efforts
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 Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))
E6	NON-CORE	Validate target and collection requests
E5	CORE	Verify Operational Technology (OT) (e.g. Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS))

CYBERSPACE OPERATIONS

Paygrade	Task Type	Task Statements
E7	CORE	Allocate resources to support Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
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 (TTP) on a specific target
E4	CORE	Brief operational and intelligence updates
E4	CORE	Collect host and network data
E4	CORE	Communicate with intelligence analysts and targeting organizations
E7	CORE	Conduct capabilities management
E6	CORE	Conduct cyberspace engagement

CYBERSPACE OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Confirm authorities and Standing Rules of Engagement (SROE) for Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) planning
E7	CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO)
E7	NON-CORE	Coordinate Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners
E4	NON-CORE	Create target and collection requests
E6	CORE	Cross-check operational performance indicators (e.g., Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.)
E7	CORE	Develop operational partnerships
E5	CORE	Evaluate defense posture
E6	CORE	Evaluate mission impact of tools and techniques on specific targets
E5	CORE	Evaluate operational documents
E4	CORE	Initiate Requests for Information (RFI)
E6	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
E4	NON-CORE	Perform Cyberspace Threat Hunting (CTH)
E4	CORE	Perform host enumeration
E4	CORE	Perform network enumeration
E4	CORE	Perform network reconnaissance
E4	NON-CORE	Perform offensive tactics in support of Defensive Cyberspace Operations (DCO)
E5	CORE	Perform operational and tactical deconfliction
E4	CORE	Perform scanning activity
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.)
E4	CORE	Provide input for organic products (e.g., reports, working aids, Concept of Operations (CONOPS), etc.)
E4	NON-CORE	Provide target Positive Identification (PID)
E4	CORE	Provide time sensitive reporting information (e.g., Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIR), voice reports, etc.)
E4	CORE	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities
E4	CORE	Recognize Mission Relevant Terrain in Cyberspace (MRT-C)
E5	CORE	Relayed Defensive Cyberspace Operations/Offensive Cyberspace Operations (DCO/OCO) updates

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	Support mission analysis
E7	CORE	Validate operational documents
E7	CORE	Validate target development recommendations
E5	CORE	Verify Mission Relevant Terrain in Cyberspace (MRT-C)
E4	CORE	Verify operational authorities
E5	CORE	Verify operational environments for key terrain in cyberspace

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