2021-2023 EDUCATIONAL SKILL REQUIREMENTS
Network Operations and Technology
Subspecialty: 6209
Curriculum: 386

1. Curriculum Number: 386

2. Curriculum Length in Months: 21

3. GRE/GMAT Required: No

4. APC Required: 334

5. The officer must understand the fundamental concepts and be familiar with the basic functional areas of Network Operations and Technology within the Department of the Navy (DoN) and the DoD including:

6. ESR-1: Graduates will be able to identify and describe theories and concepts associated with data, information, information systems and networks (human and technological). They will demonstrate the ability to apply theories and technology associated with the physical information and cognitive domains to enhance and improve military operations and decision-making processes. Graduates will possess domain specific knowledge in Network Operations and the theories and technologies that enable networked military operations.

7. ESR-2: The following common core knowledge areas will be common to all officers earning the 6209 subspecialty code:

a. Computing and networking theory and applications to include cloud computing concepts, "Big Data" management and applications, RF-based and mobile telecommunications;

b. Cybersecurity and Information Assurance (IA) theory, applications, and emerging capabilities;

c. Network, enterprise, systems, and software architecture, policy, security, and life-cycle management theory and applications;

d. Information theory and data-centric implications in the military environment to include a survey of Information Management, and Data Science concepts and approaches;

e. Analytical Decision Making and Process Change Management.

8. ESR-3: Graduates will possess the skills to be able to:

a. Compare and evaluate existing, emerging and innovative technological and theoretical approaches to military operations in terms of how information is acquired, processed, stored, transmitted, managed, protected, organized, displayed, and ultimately used.

This includes understanding the application of these areas as they apply to concepts of observation, orientation, decisions and ultimately actions in the battlespace.

b. Evaluate and critique existing information policies, procedures and doctrine affecting military operations, and propose alternatives to seize and maintain information advantage. This includes security policies and those impacting the authenticity, availability, confidentiality, integrity, and non-repudiation of information.

c. Optimize information warfare system configurations to align with changes in the operational environment and understand the critical nature of information in military planning and operations. This includes concepts associated with cloud computing, big data, emerging media, and various transmission capabilities.

d. Develop and manage the implementation of Information Assurance and computer security policies appropriate for the operational environment and current regulations.

e. Conduct independent research. Students will demonstrate their ability to incorporate concepts learned in the Common Core and their Specialized Track by completing either a group research project or individual thesis. The group research project (i.e., practicum) or individual thesis research will be conducted in an area relevant to current Navy priorities and strategy. In addition to completing a written project report or individual thesis, each student will demonstrate knowledge and skills through an oral presentation of their research.

9. ESR-4: Specialized Tracks: Each graduate will complete courses related to one of two specialized areas of interest to Network Operations and Technology: Information Dominance Operations and Information Systems Management.

a. Track 1: Information Warfare Operations (IWO): Integrate and synthesize information warfare maneuver to include a survey of advanced sensing, robotics, unmanned systems, industrial and control systems networks, artificial intelligence, machine learning, and big data analytics. Learning emphasis will be on theories and principles of information and data science in Command and Control (C2) denied and degraded environments. This track includes a capstone course designed to integrate concepts of information warfare in a joint and maritime environment. Graduates of the IWO track will be able to relate existing concepts of operational art, information theories, and information systems technologies to current and emerging military problem sets. To this end, graduates will demonstrate the ability to:

(1) Identify elements of Assured C2 and identify means to achieving Assured C2 throughout the Navy. This includes an understanding of the constituent components (e.g., resources, requirements, capabilities, governance, tactics, techniques and procedures) that must be marshaled and aligned with doctrine, organizational structure, training, material, logistics, personnel and facilities to achieve optimal effect.

(2) Optimize information/C2 systems configurations to align with emergent and anticipated changes in the operational environment to support decision maker needs including satellite and space communications systems, Positioning, Navigation and Timing (PNT), and space-based sensing capabilities and applications.

(3) Identify resilient C2 configuration plans to cope with natural and human-induced changes in communication channel capacity and the information environment in general. These changes include but are not limited to anti-access/area denial situations, emission control and Electromagnetic Maneuver Warfare (EMW) requirements, satellite loss and/or degradation, intruded, degraded or compromised networks (to include – Denied Disconnected, Intermittent and Limited (D-DIL) bandwidth environments), varied terrestrial, celestial and meteorological environments.

(4) Evaluate ship, shore, airborne, expeditionary, National information warfare capabilities (to include DoD Information Networks (DODIN)), Radio Frequency (RF) theory, and electromagnetic spectrum usage and protection.

b. Track 2: Information Systems Management (ISM): This track focuses on the systems engineering, acquisition and program management of Information Technology (IT) in support of sustainment to global and collaborative military operations while accounting for concepts and technologies used to achieve confidentiality, integrity, and authenticity for information processed across networks. Students will examine modern industry trends, human factors, methods/policies, enterprise investment strategies, information security and risk management considerations, system analysis, analytics, and design as they apply to information systems. Graduates will understand how to develop appropriate technical and acquisition plans and policies, perform financial, cost-benefit and trade-off analyses, and execute required lifecycle planning, programming, and budgeting actions for an IT enterprise that supports National Security Strategy. To this end, graduates will demonstrate the ability to:

(1) Plan and manage an information technology project/program including required planning, programming and budgeting actions. Understand how to exploit technology advantages in a network-centric environment to achieve operational objectives.

(2) Effectively manage information system assets through a thorough understanding of systems engineering, managerial concepts, evaluation techniques, systems analysis and design, which involves adapting to technological, organizational, and economic changes.

10. Curriculum Sponsor, Major Area Sponsor and Subject Matter Experts:

a. Curriculum Sponsor: [redacted]

b. Major Area Sponsor: [redacted]

c. Subject Matter Expert: [redacted]

d. Action Officer SME: [redacted]

APPROVED: [redacted]

APPROVED: [redacted]

APPROVED: [redacted]

APPROVED: [redacted]