Proposed FY16-18 Educational Skill Requirements
Cyber Systems and Operations (CSO)
Subspecialty 6208
Curriculum# 326

1. Curriculum Number: 326

2. Curriculum taught at NPS.

3. Students are Fully Funded.

4. Curriculum Length in Months: 21 with or without JPME

5. APC Required: 334

6. The CSO curriculum uniquely prepares Officers with the educational background, problem solving, and critical thinking skills to serve in challenging Cyberspace Operations and Cyber Warfare key leadership, operational planning, systems management, and Cyber capability employment positions within the military. The program couples the factors of decision-making, operational warfare context, and technical specialization based in the disciplines of computer science, information sciences, electrical engineering, and emerging Cyber academic programs. The CSO curriculum includes emphasis on means to support the Information Dominance pillars of Assured Command and Control, Battlespace Awareness, and Integrated Fires. The program directly supports Navy, USMC, and DoD goals of operating the network as a warfighting platform, delivering warfighting effects through cyberspace, creating shared cyber situational awareness, and aiding in maturing of Cyber Mission Forces.

a. Cyberspace Operations (CO) Foundations. Graduates of the CSO program will: have acquired knowledge of Cyber Warfare and Cyberspace Operations concepts and methodologies; demonstrate a proficient application of the technical dimensions of Cyberspace Operations; and be able to analyze, synthesize and evaluate management, engineering, and operational approaches to solve complex problems within Cyber Warfare. This foundation must provide graduates who possess the educational skills to:

(1) Develop and execute well-formed strategies and plans to effectively operate and maintain ready information and control networks supporting military operations.

(2) Develop and execute best practices and methodologies for effective Defensive Cyberspace Operations (DCO) to include assessment of threat vectors and vulnerability assessment, means to mitigate cyber attacks and exploitation through active defense, and network maneuver methodologies.

(3) Build and assess disparate behaviors and indicators within cyberspace to ascertain Cyber Intelligence supporting military operations.

(4) Define, identify, and assess Cyber Key Terrain from within supporting System of Systems and associated functional processes.

(5) Be able to generate operational risk factors in support of mission assurance and cyber operations.

b. Technical Foundations. Graduates will be able to apply critical thinking, fundamental mathematical, computer science, and engineering concepts underpinning Cyberspace Operations in an operational context. In particular, graduates will be able to employ Cyberspace Operations concepts to solve operationally relevant problems. This education will be founded in the following technical areas: computer architecture; operating systems; virtualization; networking, mobile, and wireless technologies; cyber physical systems and industrial control systems; computer and network security; computer programming; reverse engineering and digital forensics; data analytics; probability; statistics; and signals operations.

c. Military Application. Officers will be able to analyze Cyber requirements within military operations and synthesize and evaluate courses of action that include the use of Cyber capabilities within the full range of military capabilities (kinetic to non-kinetic). These skills will be reinforced through the use of the Joint Operational Planning Process, Joint Targeting Cycle, Joint doctrine on Cyberspace Operations, and related operational concepts. The Officer is to build skills for the effective application of cyber capabilities, understand the implications and complexities of delivering cyber effects, and be able to integrate Cyberspace Operations within operational planning and execution processes. In particular, the Officer will be able to develop, compare, and evaluate courses of action incorporating Cyberspace Operations and identify targets and processes against which cyber capabilities can be employed to achieve operational effects in support of operational objectives.

d. Organizational Construct and Policy Context. The Officer will be able to describe the administrative and operational structure and command relationships of the organizations and commands that operate within the cyberspace domain. The Officer must have a foundational understanding of the application of DoD / DoN policies, related strategies, authorities, and the Law of Armed Conflict in the execution of Cyberspace Operations, Cyber Warfare, and associated capabilities. The Officer will be able to illustrate the employment of these organizational relationships and policy, strategy, authorities, and legal context in an operational environment (i.e., Cyberspace Operations implications from U.S. law, National Security Strategy, DoD Cyber strategies, DoD and related policies, Rules of Engagement, etc.).

e. Comprehension of the Cyberspace Environment. The Officer will understand the characteristics of friendly, neutral, and adversary Cyber environment and likely methodologies for adversary employment of cyber capabilities (e.g., infrastructure, prevalent technologies,

policy limitations or deterrence, etc.). The Officer will understand the parameters of Cyberspace Situational Awareness, methodologies for attribution, collateral damage effects, and operational risk of Cyberspace Operations. Further, the Officer will understand architecture and design principles that underpin cyberspace as well as demonstrate the ability to analyze specific cyber system implementations to identify vulnerabilities and potential attack vectors. The Officer must also understand operational implications when the environment shifts from a permissive and a contested environment.

f. Relationship to other Warfare Areas. The Officer will understand and illustrate the relationships, overlaps, and interdependencies between cyberspace and traditional warfare areas to include air, surface, undersea, amphibious, strike, and expeditionary warfare. Further, the Officer will also demonstrate understanding of relationships and interdependencies between cyberspace and space and Electromagnetic Maneuver Warfare. In particular, the Officer will be able to describe alternative approaches to conducting Cyberspace Operations within an Anti-Access/Area Denial scenario.

g. Independent Research. The Officer will demonstrate the ability to conduct independent research and investigation through completion of a thesis or a group capstone project, which meet the requirements of the conferred degree. Thesis or capstone work will be conducted in a framework that exercises the practices of innovation, critical thinking, problem solving, and real-world applicability. Where possible, the topic of the thesis or capstone project will support operational focus areas defined by the mission area sponsor. Further, the Officer will be able to present research goals and results in both written and oral form.

h. Joint Professional Military Education (JPME). Per community requirements, the Officer will have an understanding of warfighting within the context of operational art to include: strategy and war, theater security decision making, and joint maritime operations. Completing the Naval War College four-course series leading to Intermediate Level Professional Military Education and JPME phase I certification fulfills this requirement.

APPROVED:	FCC/C10F (Curriculum Sponsor)	18 JUN 15 Date
APPROVED:	OPNAV N2/N6 (MAS)	13 JUL 2015 Date
APPROVED:	President, NPS	~~JAN 15 2016~~ Date
APPROVED:	OPNAV N12 (TFMTERD)	22 Feb 2016 Date