Cyber Systems Operations (326) and Applied Cyber Operations (336) Student Orientation Brief

Program Officer: Dr. Duane Davis

25 September, 2012
• Academic and Military Information
• General Curriculum Information
• Educational Skill Requirements (ESR)s
• Matrix and Course Overview
• Cyber Wargames
• Thesis and Capstone Research
Student Services

• Student check-in / out
• Student FITREPs and Evals
• Navy required training
• Student conduct and Honor Code issues
• Housing issues
• Student mustering / announcement web page
• Overseas screenings

• Student PFA
• Student military admin (bonus / special pay, lateral transfer, special packages)
• Family Service / Family Advocacy
• Student Affairs, Orientation, Awards, graduation, ceremonies
• Mail diplomas / transcripts

Hermann Hall, Room 033, x3812 / 3813
Program Office

- Program Officer: Dr. Duane Davis, GE-309, x7980 for now—then TBD
- Ed Tech: Mrs. Maricel Eddington, GE-308, x7981

- Curriculum implementation
- Course matrix development
- Class registration
- Schedule changes

- Academic counseling
- Academic probation
- Degree nominations
- E-week tracking
Military Requirements

• Leave—"Current Students" page
  – Routed through Program Officer
  – Use NSIPS
• Special Liberty
  – PO can approve 72-hour, DoS can approve 96-hour
  – Route special request chit (form on the Admin intranet site)
  – Online "request to miss muster"
• Enrichment Week
  – After summer and winter quarters
  – Participation is mandatory, but YOU pick the events
• PFA ~ October / April

• Muster daily NLT 1000 via student check-in webpage
  – General announcements and communications
  – Fail to muster (FTM) – earn visit to DOS to explain
  – Must be in the local area!
• Check e-mail at least 2x daily
  – Specific Comms / Urinalysis
• SECNAV Guest Lectures
  – Attendance is required
  – Section Leader
• IRB
  – Human research checklist submitted with thesis proposal
  – Advisor responsible, but you may do the legwork
• Academic integrity at the Naval Postgraduate School is based on a respect for individual achievement that lies at the heart of academic culture. Every faculty member and student belongs to a community of scholars where academic integrity is a fundamental commitment.

• Academic dishonesty is not tolerated.

• Unless otherwise stated by the instructor: all in-class work submitted for a grade will be the student’s own, performed without reference to materials or other individuals.

• Graded work assigned for completion outside the classroom may allow the use of reference material (follow instructor’s instructions), but shall be performed without the assistance of other individuals. All written work should be appropriately identified referenced material.
Violations of the Honor Code may be resolved through punitive, disciplinary, or administrative action under military or civilian systems.

**Military Personnel**

- Informal counseling
- Comments on fitness reports and evaluations
- Disenrollment
- Administrative separation
- Punitive measures under UCMJ.

**Civilians**

- Informal counseling
- Comments in performance evaluations
- Disenrollment
- Disciplinary action including removal from the Federal Service
• Minimum of 4 slots filled (courses/thesis slots) per quarter required.

• Course credit vs course hours: (3-2) – 3 lecture hours/week; 2 lab hour/week; 4 credit hours (labs count as ½)

• Minimum GQPR 3.00 for 3000-4000 Level Classes.

• Minimum Overall QPR: 2.75

• Minimum Graduate QPR: 3.00

• Academic Probation when you drop below graduation minimums.
For the following quarter….

- Course registration is conducted through the first two weeks of the current quarter.
- Python is “locked” for the next quarter after the second week of the current quarter.
- See your AA for course enrollment issues during pre-registration.
For the current quarter...

- Drop requests at the beginning of the quarter are only approved under special circumstances.

- When feasible only: Add/drops can be done during the first two weeks.
  - Will NOT appear on transcript.
  - WILL show up in Python.

- “Withdrawals” accepted thru the eighth week
  - Will appear as a “W” on transcript, no QPR impact.
  - No withdrawals after the eighth week.

- Drops/Withdrawals are requests... Make no assumptions until request has final approval!
  - Poor performance / instructor preference ARE NOT criteria for a drop or withdrawal.
  - Students will continue to attend class until drop request is approved by Program Officer.
Thesis Process

• Thesis Proposal
  – Identify advisor, discuss and indentify topic, set up research plan
  – Thesis slots (CY0810): 3 slots
  – Role of Thesis Advisor ~ Academic Rigor/Depth/Scope
  – Role of Co-Advisor or 2\textsuperscript{nd} Reader ~ Readable/Sanity Check
  – Role of Department Chairman ~ Masters Level
  – Role of Program Officer ~ Military/Sponsor Relevance

• Thesis Process Time-frame
  – One year before graduation: identify topic and start work on it.
  – ADVICE: START EARLY to avoid scrambling during last quarter!
  – Goal: Finish Thesis while at NPS, AVOID thesis extensions as much as possible.
  – Likelihood of finishing exponentially decreases when leaving NPS without completed thesis.

• Last Quarter:
  – First two months of quarter only, last month used by formatting issues, etc.
  – Final draft cleared & signed by advisor and co-advisor at the beginning of last month of the quarter
  – Due in Chairman’s office at the start of last month of the quarter
Student Opinion Forms (SOFs)

• Designed to provide feedback to improve….
  – The course content and structure
  – The instructor effectiveness

• Fully Confidential
  – Instructor cannot see the SOFs until the grades have been submitted
  – Students cannot see their grades until their SOFs have been submitted

• Routing
  – Numerical marks are seen by Chair, Dean, Provost
  – Comments are seen by the Instructor only

Be constructive!
Focus on course content, structure, and instructor effectiveness only…
Other issues should be raised directly with AA and/or Program Officer.
Remember, you are Military Officers and Senior Enlisted earning a Masters’ degree—you’re not college students. Maintain your professionalism and integrity in everything you do.

You are required to read and are responsible for the following:

- Student Online Handbook
- Academic Council Policy Handbook
- Academic Honor Code Instruction
Cyber Systems Operations (CSO) and Applied Cyber Operations (MACO)

Cyber Academic Group Chair: Dr. Cynthia Irvine
Education Tech: Ms. Maricel Eddington
Program Officer: Dr. Duane Davis

CSO:
Cohort Starts: Fall/Spring
Minimum APC Requirement: 344
Duration: Six Quarters
21 Courses with JPME (not including thesis blocks and seminars)

MACO:
Cohort Starts: Fall
Minimum APC Requirement: 344
Duration: Four Quarters
14 Courses (not including capstone blocks and seminars)
MS CSO and MACO Desired Outcomes

**BLUF:** MS CSO addresses a broad range of topics needed by leaders, and operators serving military missions.

**This curriculum ensures:**
Officer readiness to take decisive actions to achieve operational success***

- Responsibilities for Naval networks
- Accountability for application of offensive & defensive cyber capabilities.
  - GIG infrastructure integration with tools & TTP’s
- Continuing to operate safely in a denied or compromised environment.

***Derived from CNO Executive Board 05JAN12

**Meet Dept of Navy Objectives for FY12 and beyond:**
Maintain Warfighter Readiness in an Era of Reduced Budgets***

- Effectively and Correctly Size the Naval Services to Meet Strategic Demands
- Organize, Train, and Equip Combat Ready Forces
- Maximize Cyberspace Operations Effectiveness
- Improve Resiliency of the Force
- Increase Safety by Preventing Personnel and Material Mishaps

***Derived from DON Memo 03JAN12
Educational Alignment to Cybersecurity Workforce Framework

National Initiative for Cybersecurity Education (NICE)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &amp; Maintain</td>
<td>Data Administration</td>
<td>Info System Security Mgt</td>
<td>Knowledge Mgt</td>
<td>Customer &amp; Tech Support</td>
<td>Network Services</td>
<td>System Administration</td>
<td>Systems Security Analysis</td>
</tr>
<tr>
<td>Protect &amp; Defend</td>
<td>Computer Network Defense (CND)</td>
<td>Incident Response</td>
<td>CND Infrastructure Support</td>
<td>Security Program Mgt</td>
<td>Vulnerability Assessment &amp; Mgt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze</td>
<td>Cyber Threat Analysis</td>
<td>Exploitation Analysis</td>
<td>All-source Analysis</td>
<td>Targets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operate &amp; Collect</td>
<td>Collection Operations</td>
<td>Cyber Operational Planning</td>
<td>Cyber Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Legal Advice &amp; Advocacy</td>
<td>Strategic Planning &amp; Policy</td>
<td>Education &amp; Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigate</td>
<td>Investigation</td>
<td>Digital Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cyber Education & Training for Cyber Workforce Level II: Leadership
Cyber Functions and Fundamentals:
- Securely Provision
- Operate and Maintain/Network Operations/DoD GIG Operations
- Active Defense/Defensive Cyberspace Operations
- Operate and Collect, Cyber Intelligence
- Analyze and Advise
- Offensive Cyberspace Operations
- Investigate
- Communications Electronic Attack
- Friendly Cyber Defense Forces
Military Applications and Cyberspace Operations:

The officer will be able to analyze cyber requirements of military operations and direct the effective employment of cyber assets in support of national and military objectives. In particular, the officer will be able to develop, compare, and evaluate courses of action for the incorporation of cyber capabilities in all CONPLAN/OPLAN stages of operation to achieve Assured C2, and maintain Freedom of Maneuver in Cyberspace, and deliver COCOM effects (including both non-kinetic effects and non-kinetic means of facilitating kinetic attack).
• Organizational Construct and Policy:
The officer will have an in-depth understanding of the administrative and operational structure and command relationships of the organizations and commands that will be operating in the cyberspace domain. Additionally, the officer will be able to recall and apply strategy, policy, and authorities (ROE, U.S. law, the Law of Armed Conflict, and national policy) as it pertains to the use of non-kinetic force.

• Cyber System Engineering:
The officer will be able to analyze existing and proposed cyber systems for the purpose of assessing cyber requirements, capabilities and limitations, identifying capability gaps, and devising system improvements. Further, the officer will be able to develop concepts of operations for new systems including integration with existing systems and assessment of test and evaluation plans.
Cyber Infrastructure within the Joint Information Environment:
The officer will understand friendly and adversarial cyber infrastructures and will be able to diagram and explain subsystem relationships, interactions, and functions. Specifically, the officer will be able to describe and critique existing and infrastructures including (1) bottom-up systems for data collection or effects delivery, (2) middleware systems for smart push/pull services in a cloud/service-oriented-architecture, (3) top-down systems for command and control with a common operational picture, and (4) core infrastructure systems providing enabling communications. Additionally, the officer will be able to analyze specific cyber system implementations to identify adaptive cyber vulnerabilities and effects for defensive and offensive operations in both permissive and contested environments. The officer will be able to apply these analytic and problem-solving skills in Joint Information Environment operations to augment manpower with automated intelligence analytics for processing high volume, heterogeneous data sets to automatically produce high value alerts and actions in support of mission objectives.
• **Space:**
The officer will understand and be able to explain the nature of Space Operations as it is applied within the realm of cyber operations. He/she will be able distinguish between the four JP 3-14 defined mission areas (Space Control, Space Support, Force Enhancement, Force Application) and interpret how current and planned space capabilities contribute to the satisfaction of these mission areas.

• **Independent Research:**
The officer will demonstrate the ability to conduct independent investigation through the completion of a thesis or capstone project. Thesis work will be conducted in a framework that exercises the practice of innovation, critical thinking, problem solving, and real-world applicability. Further, the officer will be able to present research goals and results in both written and oral form.
• 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. This requirement is fulfilled by completing the Naval War College four-course series leading to Intermediate Level Professional Military Education and JPME phase I certification.
## CSO Matrix

### Provides:
- 6208 P-Code
- Thesis
- Integrated JPME
- CY4900 Seminars
- Cyber Wargaming Graduate Certificate (*)

### Degree:
- MS-Cyber Systems and Operations

### Entrance Requirements:
- Undergrad degree with APC 344
- TS/SCI clearance

<table>
<thead>
<tr>
<th></th>
<th>CY3000 Intro to Cyber Systems and Operations (SECRET)</th>
<th>CY3100 Introduction to Communications Networks</th>
<th>CY3110 Internet Protocols</th>
<th>CS3030 Computer Architecture &amp; Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(F/Sp)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IS3502 Network Operations I</td>
<td>CS3600 Intro to Computer Security</td>
<td>CY3300 Cyber Communications Architectures (SECRET)</td>
<td>DA3105 Conflict and Cyber Space</td>
</tr>
<tr>
<td></td>
<td>(S/W)</td>
<td></td>
<td></td>
<td>CY4900 CSO Seminar</td>
</tr>
<tr>
<td>3</td>
<td>CY3602* Network Operations II</td>
<td>CY4700* Cyber Wargame: Blue Force Ops</td>
<td>CY3800 Signals Operations (TS/SCI)</td>
<td>NW3230 Strategy &amp; War</td>
</tr>
<tr>
<td></td>
<td>(F/Sp)</td>
<td></td>
<td></td>
<td>CS4900 CSO Seminar</td>
</tr>
<tr>
<td>4</td>
<td>CY0810 Thesis Research</td>
<td>CY4600 Network Ops in a Contested Environment (TS/SCI)</td>
<td>CY4400 Cyber Mission Planning (TS/SCI)</td>
<td>NW3285 TSDM</td>
</tr>
<tr>
<td></td>
<td>(S/W)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CY0810 Thesis Research</td>
<td>CY4650 Information Management for Cyber Ops</td>
<td>CY4710* Cyber Wargame: Red Force Ops</td>
<td>NW3275 JMO I</td>
</tr>
<tr>
<td></td>
<td>(F/Sp)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>CY0810 Thesis Research</td>
<td>CY4750 Advanced Cyber Systems and Operations (TS/SCI)</td>
<td>CY4410 Cyber Policy &amp; Strategy (TS/SCI)</td>
<td>NW3276 JMO II</td>
</tr>
<tr>
<td></td>
<td>(S/W)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Mission
- Infrastructure/Technical
- Policy/Ethics/Management
- JPME
- Thesis/Research
MACO ESRs

• Most ESRs the same as (or close to) those for CSO
  – Cyber Fundamentals
  – Military Applications and Cyberspace Operations
  – Organizational Constructs
  – Cyber Infrastructure in the Joint Information Environment
  – Academic Research

• A few CSO ESRs do not apply to MACO
  – Space
  – Organizational Construct and Policy
  – JPME
• **Cyber Infrastructure, Security, and Compliance**

The graduate will be able to combine analytical methods with technical expertise and operational experience for effective utilization of the Global Information Grid (GIG) within the following areas: provide hardware and software support to multi-media Automated Information Systems; advise on capabilities, limitations, and conditions of equipment; implement production control procedures including input/output quality control support; implement and monitor security procedures; understand and advise on assigned mission organization0level compliance and defense of Command, Control, Communications, Computer and Intelligence (C4I) systems. The graduate will understand the technical mechanisms and non-technical procedures associated with the enforcement of policies in cyber systems, and their synergistic relationships. Through an understanding of security threats and vulnerabilities, the graduate will be able to develop and deploy procedures for defending cyber assets.
<table>
<thead>
<tr>
<th>1 (F)</th>
<th>CY3000 Intro to Cyber Systems and Operations (SECRET)</th>
<th>CY3100 Introduction to Communications Networks</th>
<th>CY3110 Internet Protocols</th>
<th>CS3030 Computer Architecture &amp; Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (W)</td>
<td>IS3502 Network Operations I</td>
<td>CS3600* Intro to Computer Security</td>
<td>CY3300 Cyber Communications Architectures (SECRET)</td>
<td>CS3690* Network Security CY4900 CSO Seminar</td>
</tr>
<tr>
<td>3 (Sp)</td>
<td>CY3602 Network Operations II</td>
<td>CY4700 or CY4710 Cyber Wargame</td>
<td>CS3670* Secure Management of Systems</td>
<td>CY08XX Capstone Project</td>
</tr>
<tr>
<td>4 (Su)</td>
<td>CY4600 Network Ops in a Contested Environment (TS/SCI)</td>
<td>CY4410 Cyber Policy and Strategy (TS/SCI)</td>
<td>CS3695* Network Vulnerability Assessment &amp; Risk Mitigation</td>
<td>CY08XX Capstone Project</td>
</tr>
</tbody>
</table>

**Provides:**
- No P-code
- Capstone project
- CY4900 Seminar
- Cyber Security Fundamentals Graduate Certificate (*)

**Degree:**
- MS-Applied Cyber Operations

**Entrance Requirements:**
- Technical undergrad degree with APC 344
- TS/SCI clearance

**Mission**
- Infrastructure/Technical
- Policy/Ethics/Management
- JPME
- Capstone/Research
Example Scenario:

**Red Team Moves:**

**Example Sequence**
- Hack into Blue Team’s Network (including wireless)
- Hack into Common Operational Picture (COP) to spoof situational awareness status to maintain “GREEN/Normal Status” of Blue Force units
- Degrade Blue Force units

**Blue Team Moves:**

**Initial & Ongoing:**
- Tier 1: Daily IA practices
- Tier 2: Compliance metrics for Blue force units in-depth assessment, including wireless
- Tier 3: Monitor for Advanced Persistent Threat (APT) signatures (e.g. “look for” known TTP of “COP spoofing”)
- Tier 4: (research area) Be able to detect unknown APTs

**Responses to Red:** Attempt to isolate hacked areas and maintain operations
**INFRASTRUCTURE**

- **Current**: Existing labs on campus, such as Distributed-GIG Intelligence Automation Systems Lab and Cyber Battle Labs

- **Goal**: Obtain on-loan actual Naval systems from stakeholders

- **Goal**: Obtain/build simulators that learn new offensive attacks and simulate defense situational awareness using intelligence automation (research area of interest)

** USERS:**

Students, Faculty, Stakeholders (i.e., USCYBERCOM, C10F, CSFTP, C3F, NIOC San Diego, etc.) with desired resources utilized (i.e., PEO C4I, NCDOC, etc.).
Identified current Navy concerns

- **Cyber Academic Group NPS hub** to connect cyber research topics and sponsors to students and faculty
- **Capstone course research (CY4750)**
  - Topics provided by external SMEs
    - Dozens of topics expected
  - Faculty & SMEs triage topics to ~10
  - Class reduces list, form teams
    - Consult with SMEs
  - Complete work on problem in 1 quarter
- **Thesis research** integrates
  - Topics identified by external experts
    - N2N6, C10F, USCYBERCOM, NSA, NRO, ONR, NSF, DHS, iARPA, DARPA, etc.
  - Synergistic with longitudinal faculty research
    - Leverage and enhance research funding
    - Build deep expertise
    - Maintain science and technology edge