

FREQUENTLY ASKED QUESTIONS

WHAT ARE THE PREREQUISITES?

- Acceptance by the ECE Department. Process requires a sufficient background in mathematics and technical undergraduate studies. Applicants with a BSEE degree will usually satisfy the requirements.
- Command/Company Endorsement.

IS THERE A SERVICE COMMITMENT?

Students participating in a program at The Naval Postgraduate School may incur service and/or employment obligations.

WHO IS ELIGIBLE?

Applicants with a US government affiliation, government laboratory engineers, active military personnel, Navy civilians, current NPS resident students, and a limited number of contractors sponsored by Department of Defense (DOD) organizations. TS/SCI clearance is required.

WHEN DOES THE PROGRAM START?

Any quarter.

HOW LONG DOES IT TAKE TO COMPLETE?

Usually 3 or 4 quarters, depending upon elective choices.



CONTACT INFORMATION

Monique P. Fargues, Ph.D.

ECE Department
Assoc. Chair for Student
Programs
(831) 656-2859
fargues@nps.edu
ECEDL@nps.edu

For more information on the
ECE department, go to:

www.nps.edu/ece

For more information on other
NPS DL programs, go to:

www.nps.edu/dl

Produced by:
Naval Postgraduate School



Graduate Education
Advancement Center
411 Dyer Rd., Knox 120, Monterey, CA 93943

DEPARTMENT OF
ELECTRICAL and COMPUTER ENGINEERING

**GRADUATE CERTIFICATE
PROGRAM**

IN

**CYBER
WARFARE**

A DISTRIBUTED LEARNING PROGRAM



NAVAL POSTGRADUATE SCHOOL

THE PROGRAM

The Naval Postgraduate School (NPS) offers a graduate certificate program in Cyber Warfare. The program requires three courses and can be completed in three or four quarters, depending on elective choice.

The Cyber Warfare Certificate Program will provide students with a technical foundation that prepares them for assignments related to research, and management of wired and wireless cyber warfare systems.

Students will also be provided with an educational foundation that prepares them for leadership roles in the area of cyber warfare.

“I believe my academic background has prepared me for the challenges of high-level command and complex environments.”

- Gen. Keith Alexander, stand-up Commander, USCYBERCOM and NPS alumnus.

Program Overview EC

| Academic Quarter | Required Courses | Elective Courses |
|------------------|------------------|-------------------|
| Winter | EC3760 | EC4730 |
| Spring | EC4765 | EC4755/EC3730 |
| Summer | | DA3105/ CS4558 |
| Fall | | EC3750/EC3730 |

THE CURRICULUM

EC3760 Information Operations Systems (3-2)

Winter – TS/SCI

This course examines the Network-centric Environment that is the focus of the Information Operations (IO) Infrastructure with emphasis on models.

EC4765 Cyber Warfare (3-2)

Summer – TS/SCI

This course explores cyber warfare from an electrical engineering perspective. Rudimentary denial-of-service techniques through intelligent waveform-specific forms of computer network attack (CNA) are covered.

Elective Courses (Choose one)

DA3105 Conflict and Cyberspace (4-1)

Summer – UNCLAS

Examines how cyberspace can serve as a tool, target, and source of conflict for both state and non-state actors.

EC3730 Cyber Network and Physical Infrastructures (3-2)

Fall/Spring – UNCLAS

Cyber infrastructure systems and technologies of interest to the military, government and industry.

EC3750 Introduction to SIGINT Engineering (3-2)

Fall – TS/SCI

Signals intelligence systems with emphasis on means for accessing and geolocating signals of intelligence.

EC4730 Covert Communications (3-2)

Winter – UNCLAS

Information hiding in user data, protocol data, and radio, electronic, acoustic and other sensory signals.

EC4755 Net Traffic, Activity Detection, & Tracking (3-2)

Spring – UNCLAS

Network traffic characterization and management, and detection and tracking of anomalies.

CS4558 Network Traffic Analysis (3-2)

Summer – UNCLAS

Analytic techniques for network insight.

EC3970 Special Topics in Electrical Eng. (Cyber) (3-2)

Varies – UNCLAS

Cutting edge topics of interest to the community.

THE OUTCOMES

Upon completion of the Cyber Warfare Certificate Program, students will possess:

- the cognitive skills required for vulnerability evaluation and exploitation of wired and wireless communications networks and telecommunications systems and the ability to apply these skills to defend cyber systems.
- the ability to apply techniques for attacking computer and telecommunications networks.

And, depending upon elective choices,

- the ability to analyze and evaluate cyberspace activity to identify threats and respond appropriately.
- the ability to analyze, design and evaluate systems for accessing signals of intelligence value in cyberspace.
- the ability to analyze, design and evaluate systems for attack and defense of covert communications.
- the ability to analyze, design and evaluate approaches to maintaining situational awareness in cyberspace.



Space communications along with terrestrial microwave and fiber optics provide the core capability required to implement the global cyberspace network.