

# 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 or reserve 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

### Roberto Cristi, Ph.D.

ECE Department  
DL Business Manager  
(831) 656-2223  
rcristi@nps.edu

### Monique P. Fargues, Ph.D.

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

For more information on the  
ECE department, go to:

[www.nps.edu/ece](http://www.nps.edu/ece)

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

[www.nps.edu/dl](http://www.nps.edu/dl)

Produced by:  
Naval Postgraduate School



Center for Educational  
Design, Development, and Distribution  
411 Dyer Rd., Knox 120, Monterey, CA 93943



DEPARTMENT OF  
ELECTRICAL and COMPUTER ENGINEERING

GRADUATE CERTIFICATE  
PROGRAM

IN

CYBER  
SYSTEMS

A DISTRIBUTED LEARNING PROGRAM



NAVAL POSTGRADUATE SCHOOL

## THE PROGRAM

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

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

Students will also be provided with an educational foundation that prepares them for leadership roles in the design, procurement and management of cyber operations and systems.

**“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

Academic Quarter	Required Courses	Elective Courses
Winter	EC3730	EC4770
Spring		EC4755
Summer	EC3740	EC4715
Fall		EC4790 EC4730

## THE CURRICULUM

### EC3730 Cyber Network and Physical Infrastructures (3-2)

A survey of cyber infrastructure systems and technologies of interest to the military, government and industry.

### EC3740 Principles of Reverse Engineering (3-2)

Presents fundamental, systems-level concepts for developing an understanding of system functionality - with an emphasis on hardware systems - without a prior access to the system's design specifications.

### Elective Courses (Choose one)

#### EC4770 Wireless Communications Network Security (3-2)

Examines the impact of the radio frequency environment on the security of wireless communications networks. Specifically, considers access and availability issues related to jamming and associated countermeasures such as spread spectrum transmission.

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

This course covers network traffic characterization, traffic engineering and management, and detection and tracking of traffic anomalies with a focus on statistical and information theoretic concepts, signal processing, and control theory.

#### EC4715 Cyber Systems Vulnerabilities and Risk Assessment (4-1)

The course utilizes reverse engineering principles to identify and assess vulnerabilities in electronic, communication, and control systems and analyze risk to provide tradeoffs.

#### EC4790 Cyber Architectures and Engineering (3-2)

The course addresses the holistic design, analysis and integration of the three-tiered cyber architecture of the medium, network, and services.

#### EC4730 Covert Communications (3-2)

Electronic signal and data communication mechanisms in which the presence of a message being transmitted is concealed in plain sight of other signals or data are presented. Information hiding in user data, protocol data, and radio, electronic, acoustic and other sensory signals is examined.

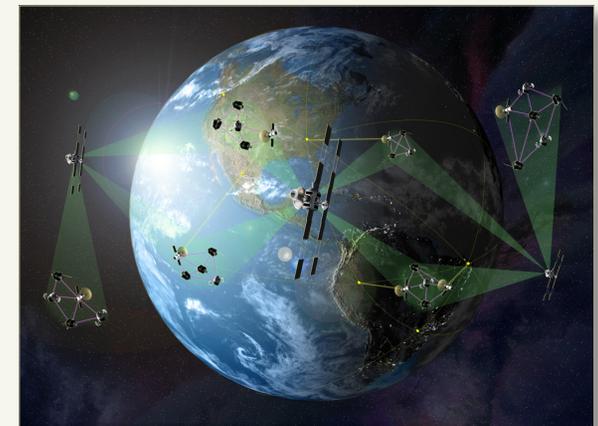
## THE OUTCOMES

Upon completion of the Cyber Systems 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.