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?
Per OPNAVINST 1520.23C, a naval officer will incur a 1 year service obligation upon completion or withdrawal from the Certificate Program, which is served concurrently with any other service obligation. All students must submit a signed Participation Agreement prior to enrolling in the program.

WHO IS ELIGIBLE?
Applicants with a US government affiliation, government laboratory engineers, active or reserve military personnel, naval 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

For more information on other NPS DL programs, go to:
www.nps.edu/dl
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**

<table>
<thead>
<tr>
<th>Academic Quarter</th>
<th>Required Courses</th>
<th>Elective Courses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winter</td>
<td>EC3740</td>
<td></td>
</tr>
<tr>
<td>Spring</td>
<td>EC3730</td>
<td>EC4755</td>
</tr>
<tr>
<td>Summer</td>
<td></td>
<td>EC4715</td>
</tr>
<tr>
<td>Fall</td>
<td>EC3730</td>
<td>EC4790</td>
</tr>
</tbody>
</table>

**THE CURRICULUM**

**EC3730 Cyber Network and Physical Infrastructures (3-2) Winter**
A survey of cyber infrastructure systems and technologies of interest to the military, government and industry.

**EC3740 Principles of Reverse Engineering (3-2) Summer**
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)**

**EC4715 Cyber Systems Vulnerabilities and Risk Assessment (4-1) Summer**
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) Fall**
The course addresses the holistic design, analysis and integration of the three-tiered cyber architecture of the medium, network, and services.

**EC4755 Network Traffic, Activity Detection, and Tracking (3-2) Spring**
Network traffic characterization, traffic engineering/management and detection and tracking of traffic anomalies are covered with a focus on statistical and information theoretic concepts, signal processing, and control theory.

**THE OUTCOMES**

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

- the cognitive skills required for reverse engineering, analysis, design and evaluation of cyber systems and infrastructures.

- the ability to apply techniques for managing supply chain risk for cyber systems.

And, depending upon elective choices,

- the ability to discover, assess and mitigate cyber system risks and vulnerabilities.

- the ability to design and evaluate cyber system architectures.

- the cognitive skills required for analysis, design and evaluation of approaches to maintaining situational awareness in cyber systems.