

ICW IDE CYBER WARFARE PROGRAM GUIDE

1. Introduction

The Intermediate Developmental Education (IDE) Cyber Warfare (ICW) program is designed to develop technical and leadership expertise in cyber warfare and cyber operations, in keeping with the USAF vision to “Deliver sovereign options for the defense of the United States of America, and its global interests – in air, space, and cyberspace.”

Although the definition of cyberspace varies, for the purposes of this program, it includes the electronic realm in which information is stored, processed, and transmitted, to include computer networks and equipment, storage media, and free space. Studies in cyber warfare then would include education and research into the protection of friendly operations in cyberspace, coupled with the attack against or disruption of adversary capabilities. Ultimately it is a question of how best to apply cyber power (offensive and defensive) in order to achieve strategic and operational military objectives.

Cyber operations is closely tied to the field of information operations, and doctrinal discussions and definitions are quite fluid at this point in time. The challenge is that both cyber and information operations deal with *information* (knowledge, content and cognition) and *information systems* (computers, networks, and communication systems). It is becoming more and more difficult (and perhaps ill advised) to separate these concepts, since “information dominance” can be achieved through a combination of attacking and/or defending both the information and the systems.

As such, this program of study which include a wide variety of disciplines that includes both technical and nontechnical aspects, to include the following:

- Influence operations, psychological operations, and deception
- Command and control warfare
- Electronic warfare
- Electronic sensors
- Communications systems and networks
- Computer and network security
- Threat / vulnerability assessments and risk management
- Legal / ethical aspects of cyber warfare
- Strategic and tactical planning for cyber operations and warfare

2. Objective

The objective is to develop a broad background in cyber warfare theory/application, thereby providing graduates with a foundation to better understand, develop, acquire, manage and employ cyber-based capabilities now and in the future. Due to the length of the program and

the nature of the target audience, emphasis is on breadth rather than technical depth. The program typically leads to the Master of Cyber Warfare degree.

3. Entry requirements

This degree program is only available to officers selected by the Air Force Personnel Center (AFPC) for the in-residence IDE degree program. This program is not strictly limited to technical officers. However, students will need to be comfortable with advanced topics in computers and communications systems. Candidates with a bachelor's degree in computer science, engineering, math, or physical sciences with an above average GPA (3.0+) should have few problems with the program. Students with the following will also be considered:

- Bachelor's degree with an above average GPA (3.0+) and one year of college level mathematics (algebra, calculus, linear algebra)
- Significant information technology (IT)-related work experience (programming, network operations, systems acquisition)
- Operational experience in various cyber war activities, such as network operations, electronic warfare, C4ISR, systems acquisition

4. Program Requirements

The ICW program curriculum consists of the following components: (1) core sequence, (2) application sequence, (3) mathematics requirement, and (4) a Graduate Warfighting Project (GRP), each of which are further described below.

Any course substitution or change in the ICW program requires approval from the head of the Department of Electrical and Computer Engineering.

a. Core Sequence (16 quarter hours)

The objective of the core courses is to provide a strong foundation in cyber / information warfare theory, doctrine, capabilities, vulnerabilities, threats, and risk management.

CSCE 525	Introduction to Information Warfare (4)
CSCE 560	Introduction to Computer Networks (4)
EENG 509	Fundamentals of Electronic Warfare (4)
IMGT 687	Managerial Aspects of Information Warfare (4)

b. Application Sequence (20 quarter hours)

The application sequence builds on the core sequence by providing the student with an opportunity to apply knowledge to real-world scenarios, as well as synthesize new ideas for how cyber power can be applied to meet strategic and operational military objectives.

OPER 501	Quantitative Decision Making (3)
CSCE 528	Cyber Defense and Exploitation I (4)

CSCE 628	Cyber Defense and Exploitation II (4)
CSCE 629	Network Attack and Exploitation (4)
CSCE 729	Cyber Operations Capstone (4)
CSCE 699	Cyber Operations Seminar (1)

c. Math Requirement (4 quarter hours)

Students are required to take at least one course in graduate mathematics or math science. In addition to courses offered by the Department of Mathematics and Statistics (MATH/STAT), the following courses may also be used to satisfy this requirement:

CSCE 531	Discrete Mathematics (4)
CSCE 554	Fundamentals of Performance Analysis and Experimental Design (4)

d. Graduate Research Project (GRP) (8 quarter hours)

All students are required to complete a graduate warfighting project under the direction of a faculty advisor. Similar in objective to an AFIT Master of Science (MS) thesis, the GRP involves significant academic research or design effort. The GRP reflects a high level of competence a student has attained as a candidate for a degree. It demonstrates knowledge, understanding, originality and independence in selecting and approaching a problem, skill in planning and accomplishing a research or design effort, the capacity to work in teams and the ability to communicate orally and in writing. Most importantly, the GRP demonstrates the application of the student's field of study and will exercise the graduate student's ability to apply the scientific method and/or apply engineering and mathematical tools and models to solve real problems.

The GRP topic is normally broad in scope, Air Force and/or DoD focused, and may require a variety of backgrounds, experience and academic program disciplines to adequately address complex problems. Students will select an area of research or design, or may be assigned, based on their academic program. The project is normally completed by groups of students and provides an introduction to the research process, strengthens the student's writing skills, and augments the AFIT research program. The project is documented in an advisor-approved format and presented orally.

Sample ICW Program

1st Quarter – Summer

CSCE 525 Introduction to Information Warfare
STAT 525 Applied Stats for Managers
OPER 501 Quantitative Decision Making

2nd Quarter – Fall

CSCE 560 Intro To Comp Networking
CSCE 699 Cyber Operations Seminar
EENG 509 Fundamentals of Electronic Warfare
IMGT 687 Managerial Aspects of Information Warfare

3rd Quarter – Winter

CSCE 629 Computer Network Attack / Exploitation
CSCE 528 Cyber Defense and Exploitation I
CSCE 798 Graduate Warfighter Project

4th Quarter – Spring

CSCE 628 Cyber Defense and Exploitation II
CSCE 729 Cyber Operations Capstone
CSCE 798 Graduate Warfighter Project