**Air Force Institute of Technology**

**Department of Electrical and Computer Engineering**

**CSCE 525: Introduction to Cyber Warfare and Security**

Fall Quarter 2018

Syllabus

**Instructor:** Lt Col Mark Reith

[mark.reith@afit.edu](mailto:mark.reith@afit.edu)

Building 642, Room 207

255-3636 ext 4603

**Class Meetings:** 1000 - 1200, Monday & Wednesday

Building 640, Room 338

**Office Hours:** By appointment (email preferred). I have an open door policy, so please feel free to drop by anytime. If I’m busy, we can make an appointment.

**Text/Materials:** Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Second Edition by Jason Andress & Steve Winterfeld; other readings as assigned.

Research Methods for Cyber Security by David Manz & Thomas Edgar (optional)

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2nd Edition by Michael N. Schmitt (optional)

**Prerequisites:** None.

**Credit Hours:** 4 hours.

**Course Description:** This course studies the nature of Cyber Warfare and its ramifications for information system security and survivability, and information assurance. It provides a foundational understanding of operational considerations, tactical capabilities, limitations, strategic ramifications, policy, and legal guidelines associated with offensive and defensive cyberspace operations. Simultaneously, it engenders a systems-oriented viewpoint, while examining national information infrastructures, their vulnerabilities, interdependencies, threats, and opportunities for exploitation.

**Course Objectives:**  This course studies the nature of information assurance, information operations, information warfare and their ramifications for military operations and national security. Emphasis is on cyber warfare and operations in cyberspace across the major phases of conflict. Major topics include an overview of cyber defense, fundamental security principles, legal concerns, risk management, cyber-physical linkages to include industrial control systems and embedded systems within vehicles, and finally cyber-operational linkages to include multi-domain operations and mission assurance.

Students are expected to complete the course with a working knowledge and understanding of cyber operations and their impact on warfare and national security. Students will possess a foundational understanding of cyber security principles and methods and technologies for defending systems and networks. Students will understand the relationship between vulnerabilities, exploits and threats, as well as a frameworks for assessing risk. Students will understand the current legal framework governing cyber operations. Students will understand cyber-physical and cyber-operational linkages to include industrial control systems. Students are expected to demonstrate critical thinking and communication through graded deliverables and class participation.

**Grading:** Research Paper: 40%

Teaching Video: 30%

Critical Thinking Checks: 20%

Class Participation: 10%

Final course grades will be based on the following scale:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **A-** | **B+** | **B** | **B-** | **C+** | **C** | **C-** | **D** | **F** |
| **93+** | **90+** | **87+** | **83+** | **80+** | **77+** | **73+** | **70+** | **65+** | **<65** |

**Research Paper:** Each student will identify a core cyber problem, assess various solutions, assert a position and write a research paper supporting their claim.  Cite research from quality academic papers and consider using real-world data sets and subject matter expertise as supporting material.  Target a specific academic conference and format your paper according to their style guidelines, otherwise follow the Air University Style & Author Guide.  Topics and conferences must be pre-approved in writing by your instructor.  Highly recommend submitting quality drafts for instructor feedback.  A list of potential topic ideas and suggestions for completing the paper will be provided.

**Teaching Video:** Each student will create a high-quality 10-20 minute video explaining one or more advanced cyber topics.  Topics must be prior approved by the instructor in writing.  You may choose to use slides or not, but ensure that visual elements clearly convey ideas and keep the audience engaged.  The purpose of this video is to demonstrate mastery of a cyber topic and to meaningfully enrich this course for other students.  This video may be presented to the class and may be posted as online content. A list of potential topic ideas and suggestions for completing the project will be provided.

**Critical Thinking:** Critical Thinking Checks (CTC) will be assigned, collected, and graded. Students may discuss general approaches answering these CTCs among themselves. The actual solutions that are turned in for grading are expected to be the original work of the individual student. Students are expected to draft a response consisting of 300-350 words as well as two references. References should follow the Air University Style & Author Guide. Assignments not turned in at the beginning of class on the day due may incur a late penalty or not be accepted depending on the situation. Submissions must be emailed to the instructor with the subject line: “CSCE 525 – CTC #”, replacing the # with the lesson number (reference Course Schedule).

**Article Critique:** Students may voluntarily and optionally chose to satisfy a CTC requirement by locating a cyber related news article, book chapter, video or paper (henceforth referred to as an artifact), and provide a critique of this artifact. To get credit for the CTC, the student must link the artifact to the Cyber Education Hub and post the critique in the comments section of this artifact. Just to be clear, you’ll need to complete a CTC or Article Critique (one or the other), but not necessary to do both. Please note that these comments may be visible to DoD employees/contractors with common access cards.

**Class Participation:** Each student will materially participate and interact with fellow students in discussions, activities and academic game play.

**Syllabus Schedule:** See attached spreadsheet for details. In general, students should expect to read one chapter of the textbook per class session along with other multimedia as assigned.

**Academic Integrity**: All students must adhere to the highest standards of academic integrity. Students are prohibited from engaging in plagiarism, cheating, misrepresentation, or any other act constituting a lack of academic integrity. Failure on the part of any individual to practice academic integrity is not condoned and will not be tolerated. Individuals who violate this policy are subject to adverse administrative action including disenrollment from school and disciplinary action. Individuals subject to the Uniform Code of Military Justice may be prosecuted under the UCMJ. Violations by government civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (References: Student Handbook, ENOI 36 – 107, *Academic Integrity*)

**Attendance Policy**: Attendance at all class sessions and exams is mandatory for military and civilians assigned to AFIT as full-time students except for extenuating circumstances. Part-time students are expected to attend scheduled classes, and absences should be explained to the instructor. The student should provide advance notice, if possible. Scheduled classes and exams are defined by the instructor and they are documented in the course schedule. (References: Student Handbook, Graduate School Catalog)

**Academic Grievance:** AFIT and the Graduate School of Engineering and Management affirm the right of each student to resolve grievances with the Institution. Students are guaranteed the right of fair hearing and appeal in all matters of judgment of academic performance. Procedures are detailed in ENOI 36 – 138, *Student Academic Performance Appeals*.

**Testing Policy:** No formal mid-term or final exams. Mastery of content will be assessed through an academic research paper, a teaching video and online/classroom participation.

**Late Assignments:** Students should expect a 10 point penalty for every day late unless otherwise negotiated with the instructor. The instructor reserves the right to refuse grading any work that is excessively late based on circumstances.

**Communications:** When sending email correspondence, please consider starting the subject line with “CSCE 525 - ” followed by your subject topic so that I may more quickly locate your note.

**Research:** Please observe that you may be offered to participate in one or more surveys and or interviews involving the activities within this class. These surveys/interviews are important feedback to improve the quality of cyber education at AFIT and across the Air Force. You may decline to participate in these surveys for any reason and at any time without impact to your course grade. If you do chose to participate, please provide genuine and thoughtful answers. Any data or metrics collected will not be directly attributed to you in research papers, but any comments or videos posted on the Cyber Education Hub may be visible to DoD employees and contractors, and as such may be attributable. This research has been exempted from an Institutional Review Board and documentation can be provided upon request.

**Student Acknowledgement:**

I have reviewed the course syllabus and schedule, and I understand the course objectives and requirements.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date