College of Humanities and Fine Arts

Department of Politics

**COURSE ID: INTEL 410**

**COURSE NAME: Cyber Threat Intelligence**

**(Credit Hours: 3)**

Instructors: Dr. LaMesha Craft

Office: Brittan Hall, Room 343

Phone: 843-349-6634

Email: lcraft@coastal.edu

**Catalog Description**

**INTEL 410 Cyber Threat Intelligence. (3 credits)** The course provides an examination of cyber threats from state and non-state actors engaged in malicious cyber activity. Students gain a basic understanding of computer networking to identify common components of information systems, cyberspace operations terminology, and the layers of cyberspace. Students also apply analytic techniques to build situational understanding of real-world cyber threats to U.S. networks, information, and data. Through active learning techniques, students examine case studies of international cyber incidents. F, S, Su

**Course Instructional Objectives:**

The overall goal of the course is to help students increase their knowledge about the cyber threat by developing skills to conduct threat analysis using common cyber threat frameworks. Students learn skills and strategies to identify common tactics, techniques, and procedures of cyber actors as well as their intent, capability, and potential effect on U.S. national security interests. Students also identify resources (inside and outside of the Intelligence Community) for gathering the information necessary to conduct this analysis. In order to accomplish this goal, the course is designed to increase the student’s ability to:

1. Understand how cyber actors target a victim or a network.

2. Identify the primary type of cyber actors and their known and estimated intent and capability.

3. Analyze the most prominent means of exploiting vulnerabilities in cyberspace.

4. Analyze current and future U.S. and international legislation to deter and deny cyber incidents.

5. Evaluate the government and non-government organizations involved in cybersecurity and the respective expertise they provide.

 **Student Learning Outcomes:**

Upon completion of this course the student will be able to:

1. Identify the key components of computer networking and the prominent attack vectors used by cyber actors.

2. Apply the various cyber threat frameworks when analyzing cyber threat activity.

3. Explain the intent, capability, and potential effects of cyber actors against U.S. national interests, data, and networks.

4. Create an all-source cyber threat brief, demonstrating knowledge of the key national security issues, such as critical infrastructure, that can be exploited by cyber actors.

5. Explain how collaboration, coordination, and communication with various IC agencies, government organizations, and non-government organizations would enhance cybersecurity techniques.

**Required Course Materials:** No textbooks are required for this course. Readings and videos will be posted in Moodle that are related to the various topics covered in the course.

**Attendance:** You are required to be present in all class sessions for this course, which means that unexcused absences from classes will have a negative impact on your overall grade. **I will not be responsible for providing you with the information you miss during excused or unexcused class absences.** **You cannot make up any missed in-class graded assignments.**

CCU Policy Number STUD-SENA 332 goes on to establish "the following are considered to be valid circumstances for student absence.

1. Incapacitating illness or condition – limited to the number of absences that a faculty member determines to be a balance between accommodating the illness/condition and ensuring sufficient participation in class activities.
2. Accommodation for a disability, working in conjunction with Accessibility and Disability Services.
3. Official representation of the University (excuses for official representation of the University should be obtained from the official supervising the activity).
4. Death of a close relative.
5. Religious holidays (A list of primary sacred times for world religions can be found online at www.interfaithcalendar.org.)
6. Active military duty or assignment.
7. Official University closings.
8. Compliance with a subpoena."

**Late Assignments or Make-up Tests:** For documented excuses of types (a)-(d) above, students may be eligible for a make-up test. Any such leniency, as well as the scheduling of make-up tests, is at the instructor’s discretion. The expectation is that the student will be available to make-up the missed assignment within one week.

**Grading:**

Your grade will be calculated based on the following formula. See rubrics in Moodle for specific requirements of all assignments:

 Written Assignment 20%

 Oral Presentations 20%

 Mid-term Exam 20%

 Final Exam 20%

 Quizzes 10%

 Participation & Collaboration 10%

**The grade scale for this course is as follows:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Grade**  | **GPA**  | **Numerical Grade**  |  | **Grade**  | **GPA**  | **Numerical Grade**  |
| **A** | **4.0** | **90-100** |  | **C** | **2.0** | **70-76** |
| **B+** | **3.5** | **87-89** |  | **D+** | **1.5** | **67-69** |
| **B** | **3.0** | **80-86** |  | **D** | **1.0** | **60-66** |
| **C+** | **2.5** | **77-79** |  | **F** | **0.0** | **<60** |

**Written Assignment:** Much like oral communication, effective written communication is paramount when conveying the threat for decision and policy makers. Students will select a topic involving a current threat or emerging threat to U.S. networks, data, and information. See the instructions (which include the prescribed format) and the grading rubric on Moodle. The topic must be submitted for approval at the beginning of week 8 and the paper will be due at the beginning of week 14.

**Oral Presentations:** Communication, collaboration, and coordination are very important within the intelligence community. Moreover, peer-to-peer learning is invaluable. Students will complete two graded presentations. The first presentation will be a group assignment, based on the real-world scenario provided in class. The other will be an individual assignment based on your chosen topic. Each graded presentation includes specific requirements (see Moodle for the instructions and the rubric).

**Mid-term and Final Exams:** Students will take a comprehensive mid-term exam on *DD Month YYYY*. The schedule for the comprehensive final exam follows: *insert dates for respective sections.*

**Quizzes:** In-class quizzes will consist of 10 fill-in-the-blank and short-answer question. They will be given at the beginning of class (see dates below) as a means of ensuring that you have read, listened to, or viewed the assigned material and that you comprehend the concepts.

**Participation & Collaboration:**

Students will come to class having completed the assigned readings and prepared to participate in class discussions, practical exercises, and graded group presentations. Students who regularly participate in class by specifically applying or referencing course material will receive highest participation marks. This is the participation scale:

****

Additionally, a percentage of your overall participation grade will come from completing requirements from the cooperative huddles. You will be graded on a scale of 1 to 5 based on completing the assignment (see requirements for each huddle in Moodle).

**Classroom Conduct:** A classroom environment that is conducive to learning is essential. To that end, students are expected to maintain certain standards of conduct and manners in the classroom. This includes: arrive on time to class, stay awake and engaged, and do not interrupt the learning experience of your cohorts. Failure to adhere to this conduct will result in expulsion from the class for the day (which also means you are “absent”).

**Academic Misconduct:** Academic misconduct will not be tolerated. If you are caught committing an academic infraction, your action will be reported to the university. The Academic Integrity policy for Coastal Carolina University can be found at: http://www.coastal.edu/aic.

The *CCU Student Code of Conduct, (www.coastal.edu/judicialaffairs/codeofconduct.pdf*) provides examples of plagiarism and cheating:

a. Examples of plagiarism include but are not limited to the following:

 (i) Words, sentences, ideas, conclusions, examples and/or organization of an assignment are borrowed without proper acknowledgment from a source (for example, a book, article, electronic documents, or another student’s paper).

 (ii) A student submits another person’s work in place of his/her own.

 (iii) A student allows someone else to revise, correct, or edit an assignment without explicit permission of the instructor.

 (iv) A student submits work without proper acknowledgment from commercial firms, Web sites, fraternity or sorority files, or any other outside sources.

 (v) A student allows another person to take all or any part of a course, including quizzes, tests, and final examinations.

 (vi) A student submits any written assignments done with the assistance of another without the explicit permission of the instructor.

 (vii) A student knowingly aids another student who is engaged in plagiarism.

b. Examples of cheating include *but are not limited to* [emphasis added] the following:

 (i) A student uses unauthorized information, materials or assistance of any kind for an assignment, quiz, test, or final examination.

 (ii) A student knowingly aids another student who is engaged in cheating.

See the *Code of Conduct* for more details, as well as other cases of academic misconduct. **Simply put: Do your own work and properly credit ideas that are not your own.**

**Additional Administrative Information:** Coastal Carolina University is committed to equitable access and inclusion of individuals with disabilities in accordance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act. Individuals seeking reasonable accommodations should contact Accessibility & Disability Services (843-349-2503 or <https://www.coastal.edu/disabilityservices/>). You are solely responsible for informing me of your required accommodations in a timely manner. Likewise, if you require a different environment when taking quizzes/exams then you must make the necessary arrangements with me in the time prescribed by the Accessibility & Disability Services department.

**Closing of the University for Inclement Weather:** In the event of hazardous weather, faculty, staff, and students are requested to listen to local radio and television stations or visit the Coastal Carolina University website for official University closing announcements. Announcements about hazardous weather are also posted on the University’s homepage.

***Course Schedule***

**Week 1: U.S. National Strategy to Secure Cyberspace**

**Read:** National Cyberspace Strategy- US CERT

**Read:** Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

**Read:** 2019 National Intelligence Strategy

**Read:** Lowenthal, Ch. 1, What is Intelligence

**Access:** ICS-CERT Virtual Learning Portal (establish free username and password)

**Week 2: Roles and Responsibilities of Cybersecurity**

**Read:** Foreign Affairs, Defending a New Domain

**Read:** 2018 Department of Defense Cyber Strategy

**Read:** 2018 Extending Federal Cybersecurity to the Endpoint

**Reading Quiz #1:** Material from week 1 and week 2

**Week 3: Key Components of Computer Networking & Attack Vectors**

**Read:** Basic Networking Components

**Video:** Cybersecurity: Crash Course Computer Science #31

**Video:** Hackers & Cyber Attacks: Crash Course Computer Science #32

**Cooperative Huddle #1:** See instructions in the “Cooperative Huddles” folder in Moodle

**Week 4: Cyber Threats and the Information Environment: Global Perspective**

**Read:** RAND, Improving C2 and Situational Awareness for Operations in the Information Environment

**Read:** Iasiello, Innovations in Warfare & Strategy: Russia’s Improved Information Operations

**Reading Quiz #2:** Material from week 3 and week 4

**Professor will provide** Cyber Threat Brief

**Week 5: Basic & Diagnostic Structured Analytic Techniques**

**Read:** CIA, Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (pp. 1-14; 27-29)

**Read:** Heuer, Psychology of Intelligence Analysis (Ch. 1 and 2)

**Read:** 2018 Verizon Data Breach Investigations Report

**Cooperative Huddle #2:** See instructions in the “Cooperative Huddles” folder in Moodle

**Week 6: Cyber Threats: U.S. Critical Infrastructure (Part I)**

**Read:** Critical Infrastructure and Key Resources

**Read:** DHS, Critical Infrastructure Sectors (link)

**Read:** ICS-CERT Virtual Learning Portal, Class 100W: Operations Security for Control Systems

**Practical Application:** Introduction to real-world scenario (see “Scene Setter” folder in Moodle)

**Cooperative Huddle #3:** See instructions in the “Cooperative Huddles” folder in Moodle

**Week 7: Cyber Threat Frameworks**

**Read:** ODNI,A Common Cyber Threat Framework

**Read:** Lockheed Martin, Cyber Kill Chain

**Read:** C4ISRNet, ACARE + I

**Read:** The Diamond Model of Intrusion Analysis

**Reading Quiz #3:** Material from week 5 and week 6

**Cooperative Huddle #4:** See instructions in the “Cooperative Huddles” folder in Moodle

**Week 8: Mid-Term Exam & Paper Topic Due**

**Week 9: Cyber Threats: U.S. Critical Infrastructure (Part II)**

**Read:** ICS-CERT Virtual Learning Portal, Class 210W-01: Cybersecurity for Industrial Control Systems

**Oral Presentation #1:** ICS-SCADA Vulnerabilities across Critical Infrastructure

**Week 10: National Impacts of Cyber Criminals & Hacktivists**

**Read:** FBI, Cyber Crime

**Read:** Holt, Regulating Cyber Crime through Law Enforcement and Industry Mechanisms

**Week 11: Counterintelligence: Cyber Espionage & Insider Threats**

**Read:** Center for Development of Security Excellence website (select case studies in Moodle)

**Webinar:** CDSE, Cyber Insider Threat

**Read:** Stalans & Finn,Understanding how the Internet Facilitates Crime and Deviance

**Reading Quiz #4:** Material from weeks 9, 10, and 11

**Week 12: Cyber Threats and Emerging Technology**

**Read:** Li, Cyber Security Meets Artificial Intelligence

**Read:** Yampolskiy & Spellchecker, AI Safety and Cybersecurity: A Timeline of AI Failures

**Read:** CSIS,How 5G will Shape Innovation and Security

**Week 13: Cyber Threat Intelligence: Applying Cyber Threat Frameworks**

**Read:** FireEye, Advanced Persistent Threat Groups Overview

**Review:** ODNI,A Common Cyber Threat Framework

**Review:** Lockheed Martin, Cyber Kill Chain

**Review:** C4ISRNet, ACARE + I

**Cooperative Huddle #5:** See instructions in the “Cooperative Huddles” folder in Moodle

**Week 14: What’s Next: The Future of Cyber Threat Intelligence**

**Read:** ODNI, Cyber Threats to Elections

**Oral Presentation #2:** Individual brief based on chosen topic

**Written Assignment:** Due no later than 9am via email.

**Week 15:** Conclusion & **Final Exam**