Introduction to Cyber Warfare DSS 5305

Course Instructor Information:
Dr. Brett Morris
Email: bemorris@utep.edu
Office: Remote
Office Hours: by appointment only.

Course Meeting Information:
7 Weeks//May 13-June 30

Course Description:
Cyberspace is not a new domain. It is an old one, dating back to the origins of the telegraph. Yet the speed, quantity and efficiency with which information traverses our globe has increased enormously over the last four decades. In this course you will learn the fundamentals of what some are calling a new domain of warfare, cyberwar. We will argue over terms, we will examine concepts in the context of international relations theory, and touch on information systems and computer science. This course is designed to jump start your interest in cyberspace and position you with a solid foundation in both the literature and practical aspects of cyber studies. No prior knowledge of coding or computer science is required, only a strong desire to learn about all things cyber as it relates to national security.

This course will be comprised of video lectures, reading and writing assignments. While you might be tempted to skip over the video lectures and the readings they are designed to facilitate a deeper understanding of the material and concepts. Most importantly you must keep up to date on all assignments. It is a short course and getting behind will impede both your knowledge and your grade. You are welcome to schedule (in advance) office hours.

We will cover a very broad range of topics related to cyberspace. This course will cover everything from the history of the Internet, to Internet Governance, Networked Warfare, Cyberwar, the types of computer network operations and cases from actual cyber incidents. The goal of this course is to position you, the student, at the forefront of the cyber debate so you can find and engage the literature moving forward. It is not possible in 6 weeks to learn everything, but you will leave this course highly knowledgeable about the topics of cybersecurity and cyberwar. There is a great deal of material to cover so it is important that you learn the skill of “Harvarding” (Google it) your readings. This course will include a mid-term after the first three weeks and a final at the end. The mid-term and final will be in essay format.

You will be required to write two or three, 100-250-word summaries of cyber news stories per week and post them in the forum. This serves two purposes. First, it opens your eyes to the sheer volume of cyber news stories occurring daily. Second, it helps you hone your critical writing skills. Third, it will help you when you are answering mid-term and final-exam questions. These are not meant to be onerous, they are meant to be short and to the point. You can turn all three in on the same day or spread them out over the course of a week. Your grade for these summaries will be the best 14 out of 18 summaries. Within each summary identify the origin of the incident, level of incident, type of incident, and severity of incident.
Course Objectives:
At this conclusion of this course, students will be (better) able to:

• Explain, defend, and critique the major theoretical perspectives in the field of cyber security and warfare, along with their key characteristics;
• Use the above perspectives to describe the benefits and challenges associated with various interstate and domestic interactions in cyberspace;
• Define, explain, and apply key concepts used frequently in cyberspace;
• Express opinions with evidentiary and theoretical support respectfully (in speech and writing) on contemporary cyberwar debates (e.g., cyber war will not take place, cyberspace is an operational domain, cyber should be considered a major national security threat, deterrence in cyberspace, etc.);
• Have a deeper appreciation for the complexity of cyberspace, as well as a better understanding of how scholars and practitioners see, interpret, and research this new and evolving domain.
Course Reading Material:
For the course to function smoothly, you should complete all assigned readings before the class meeting for which they are assigned. Completing the readings (and participating online) are vital to success in this course. Students are responsible for all assigned readings, even if the material is not explicitly discussed in online lectures or discussions. Please note the instructor reserves the right to replace part of the participation grade with unannounced quizzes/ writing assignments if students are not completing the readings and contributing to class discussions.

The required books for the course are:

Recommended (But NOT Required) Books:
- Cyberpower and National Security (National Defense University) [Kindle Edition] Franklin D Kramer (Author), Stuart H Starr (Author), Larry Wentz (Author, Editor), Franklin D. Kramer (Editor), Stuart H. Starr (Editor)
  ISBN: 1597974234
All assigned readings (beyond the required textbook) will be made available electronically from the instructor. To receive a zip file containing all relevant readings please email me your name and a short statement of interest in cyber studies.

**Course Requirements:**
The following are the requirements for this course:

- **Participation (30%)**: Students will be evaluated on a) forum participation, b) news story analysis. Both are *required*. Please note that: a) viewing videos and reading, but not joining into our forum discussions and activities may still adversely affect your participation grade.
- **Mid-term Exam (20%)**: This will consist of multiple-choice, identification, and/or short essay questions. The mid-term will be given the week of June 3-9 (Week 4).
- **One cyber case analysis (20%)** 8-10-page detailed cyber incident case analysis of your choice. This page length does not include your reference page for citations. Use Times New Roman, 12pt. font, double-spaced with 1-inch margins.
- **Final Exam (cumulative, 30%)**: This exam will include multiple choice, identification, and/or short essays. The exam will be held on June 24 and will open 11:55 p.m. (CST) until June 30, 11:55 p.m. There will be no make-up exams unless extenuating circumstances are dire.
- **Extra Credit**: There will be several opportunities for extra credit. Look for them scattered throughout the syllabus.

**Course Guidelines:**
The following guidelines govern the requirements for this course:

1. Students are expected to participate actively on class forums/discussions. Discussion supplements course readings and video lectures, rather than simply repeat it and are critical to developing effective skills in debate, critical analysis and reasoning. Whether or not you participate or not, you are still responsible for the material covered each week on the syllabus and on the forum.

2. Papers are due digitally in PDF format. The paper is due on June 23rd, by 11:59pm. Late papers will be docked one full letter grade (10 percentage points) for the first day it is late, as well as an additional half-letter grade (5 percentage points) for each additional day it is late. Note that I will not accept excuses (for example, broken printers, lack of email/computer access/etc.) to justify missing the deadlines.
4. Failure to take an exam will result in a failing grade for the exam. Make-up exams may be offered, but only with the prior approval of the instructor (generally for documented, emergency situations). Students are therefore advised to take all exams on time.

5. Students are advised to keep class notes, graded papers, and copies of submitted work until final grades are distributed. Every effort will be made to ensure that assignments and exams are graded fairly and objectively. During the semester, please contact the instructor if you have questions regarding a grade that you received. Students with such questions should contact the instructor no sooner than 48 hours – but no later than two weeks – after receiving the grade in question. The former permits you time to think about any comments you received and formulate the justification for your inquiry. The latter ensures that we address concerns together in an expeditious manner.

6. It is the policy and practice of the University to create an inclusive learning environment. Students requiring accommodations (concerning the course meetings, material, exams, or assignments) should discuss such matters with the instructor at the outset of the course. Students are also encouraged to register with the Disability Resource Center (phone/email/web address).

7. Any exceptions or modifications to the above rules (or syllabus) are given at the instructor’s discretion, only with prior approval and only under instances of extreme emergency or serious illness. Appropriate documentation must be supplied by the student in any event of exception. (NOTE: In the case of serious illness, “appropriate documentation” means a doctor’s note indicating an illness, not just a medical visit verification form.)
Grade Distribution

<table>
<thead>
<tr>
<th>Grade</th>
<th>Score Range</th>
<th>Grade</th>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>97.00-100.00</td>
<td>C+</td>
<td>77.00-79.99</td>
<td>F</td>
</tr>
<tr>
<td>A</td>
<td>93.00-96.99</td>
<td>C</td>
<td>73.00-76.99</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>90.00-92.99</td>
<td>C</td>
<td>70.00-72.99</td>
<td></td>
</tr>
<tr>
<td>B+</td>
<td>87.00-89.99</td>
<td>D+</td>
<td>67.00-69.99</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>83.00-86.99</td>
<td>D</td>
<td>63.00-66.99</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>80.00-82.99</td>
<td>D</td>
<td>60.00-62.99</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: Any student that withdraws from the course and is failing the course at the time of withdrawal will be assigned a withdrawal-failing (WF) grade.

Academic Dishonesty:
As a University student, you have agreed to follow the University’s academic honesty policy (including policies that cover plagiarism; for more information, [http://sa.utep.edu/oscr/academic-integrity/](http://sa.utep.edu/oscr/academic-integrity/)). Students are responsible for informing themselves about these standards before performing any academic work and may direct specific questions they have regarding the policy (or its application to course assignments) to the instructor.

Schedule/Topics:
The following pages contain a general plan for the course; deviations announced to the class by the instructor may be necessary (to best meet the needs of the students and course). Required readings are marked with an asterisk (*) and are included in the textbook and are largely in order within the textbook itself. Content not in the textbook will be provided on the class portal page.

Week 1

**Wednesday - History of Cyber and RMA**
- Michael Warner, *Cybersecurity: A Pre-history*, Intelligence and National Security 27, Iss. 5, 2012

**Friday - History of the Internet**
Week 2

Monday - Internet Governance

Wednesday - Internet Governance Continued
• ICANN and internet governance sorting through the debris of ‘self-regulation’, Milton Mueller

Friday - Cybersecurity and National Security
• Chapter 1 & 2: The Decision to Attack - Brantly
• Chapter 1 & 2: Cyberspace in War and Peace Libicki
• Chapter 8 (Demchak) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World

Week 3

Monday - Military and National Security Concepts and Influence for Cyber
• Skim: Memorandum for Chiefs of the Military Service Commanders of the Combatant Commands Directors of the Joint Staff Directorates - Subject: Joint Terminology for Cyberspace Operations
• Chapters 4, 5, and 6 Brantly
• Chapter 11 Libicki
• Defense Department Strategy for Operating in Cyberspace

Wednesday - War in Cyberspace
• Chapters 12 through 19 Libicki
• Chapter 7 Brantly

Friday - The Debate
• Maj Sean C. Butler, USAF, Refocusing Cyber Warfare Thought • Thomas Rid, Cyber War Will Not Take Place
• John Stone, Cyber War Will Take Place!
**Week 4**

**Monday - Stuxenet (Pick 3) - The Outlier**  
- James P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War  
- Ralph Langer, Dissecting a Cyberwarfare Weapon  
- Dale Peterson, Offensive Cyber Weapons: Construction, Development, and Employment

**Wednesday - CNA Examples (Pick 3)**  
- Chapter 8 Brantly  
- Attack on Ukrainian Power Grid: [https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf](https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf)  
- Alexander Klimburg, Mobilising Cyber Power  
- Greg Bruno, The Evolution of Cyber Warfare  
- Chapter 3 (Lin) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World

**Friday - CNE Examples**  
- Chapter 7, 8 and 9 Libicki  
- Re-read Chapter 7 Brantly  
- Jason Fritz, How China will use cyber warfare to leapfrog in military competitiveness  
- Sanjay Goel, Cyberwarfare: Connecting the dots in cyber intelligence

**Optional**  
- Magnus Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence  
- INFORMATION SECURITY Cyber Threats Facilitate Ability to Commit Economic Espionage Statement of Gregory C. Wilshusen, Director Information Security Issues

**Week 5**

**Monday - National Strategies and Defense (Pick 3)**  
• Chapter 6 (Andres) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World
• Kenneth Geers, The challenge of cyber-attack deterrence
• Chapter 21 Libicki

Wednesday - Thinking Ahead in Cyber (Pick 3)
• Chapter 7 (Cooper) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World
• Christopher Bronk, Hacking the Nation-State: Security, Information Technology and Policies of Assurance
  Ronald J. Deibert, Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace
• Chapter 6 Libicki

Friday - Cyber Terrorism
• Brantly Innovation and Adaptation in Jihadist Digital Security
• Steve Coll and Susan B. Glasser, Terrorists Turn to the Web as Base of Operations
• CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Dorothy E. Denning Georgetown University
• Chapter 4 (Bucci) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World

Week 6
Monday - Debates
• Chapters 9 and 10 Brantly
• Chapter 34 Libicki
• Timothy J. Junio, How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate

Wednesday - Debates Continued
• Chapter 32 and 33 Libicki
• Chapter 10 Reveron
• Securing Cyberspace for the 44th Presidency

Friday Human Rights
• Aaron Brantly, The Cyber Losers
• Jeffrey T. G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare
• Larry Diamond, Liberation Technology - Journal of Democracy

Week 7-- Readings and Final Exam

Monday

• Edward T. Barrett, Warfare in a new domain: the ethics of military cyber-operations

• Chapter 7: LEGAL AND ETHICAL PERSPECTIVES ON CYBERATTACK 239 in Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities
• Chapter 14 (Reveron) in Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World