**DSS 5305**
**Cyberwarfare**
**Course Syllabus**

---

**Instructor Information**
Professor: Dr. Brett Morris  
Preferred Email: use the in-class, Blackboard e-mail system for fastest response to class issues  
Other Email: bemorris@utep.edu

**Faculty Bio**
I retired from the Air Force as a colonel. My last assignment was as the Director of Research and Publication at the Air Force's Air Command and Staff College with an appointment as a professor of national and international security. This was punctuated with special duty assignments to the Middle East and Central Asia. I've served in several information related roles with the military, the State Department and the White House and was qualified as a cyberwarfare and space operator. I've also held several operational and support jobs in the Air Force.

My cyber experience began earlier. In fact, I began before that ancient movie *War Games* first aired. That’s right. My first forays into the internet involved huge, card-directed computers with tape drive memories. Dial-up modems were a huge step forward. Later, the Air Force would allow me to play with some of their toys, though I hacked less and did social engineering more.

I earned a PhD in Political Science (major field: international relations, minor fields: U.S. politics, political psychology, political communication, public administration) from the University of Alabama and hold an MA in political science from there as well as an MS in Strategic Studies from Air War College, a Master of Military Arts and Operational Sciences from ACSC, as well as an MS in International Relations and a Master of Public Administration from Troy University (European Division). I've also completed the Air Force, Army, Navy, and Marine Command and Staff College programs.

Amazingly, I did find time to have a family, though they're grown and gone, so I'm largely left with the remnants of their menagerie plus my two German Shepherds.

**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 call 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 desire to learn about all things cyber as it relates to national security.

This course includes written and video lessons, reading assignments, other writing assignments (mostly discussion board essays & news summaries), and on-line lab work. 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 broad range of topics related to cyberspace, including internet history & governance, cyberwar, cyber defense, law, ethics, and more. It is not possible in six 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 read and understand your material sooner rather than later. This course includes weekly writing, lab exercises, a mid-term, and a final.

**Course Scope**

This course applies both historical and theoretical lenses to understanding the creation and development of the information domain with an emphasis on the internet and its functioning. In this domain, it will cover issues related to national security across the span of national power (diplomatic/political, informational, military, economic = the DIME). Its aim is to develop integration of the processes, policies, threats, and opportunities to prepare those entering government service.

**Learning Objectives**

At this conclusion of this course, students will be (better) able to:

- (LO-1) Explain, defend, and critique the major theoretical perspectives in the field of cyber security and warfare, along with their key characteristics;
- (LO-2) Use the above perspectives to describe the benefits and challenges associated with various interstate and domestic interactions in cyberspace;
- (LO-3) Define, explain, and apply key concepts used frequently in cyberspace;
- (LO-4) 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.); and
- (LO-5) 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 Delivery Method**

**Reading Assignments.** Other than text that you must purchase, you can find other reading material in the weekly course modules. Your success relies heavily on your ability to read and
apply them in this course. Unless otherwise noted, you are responsible for all assigned readings, even if the material is not explicitly discussed in online lectures or discussions. 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 "Boards"

*Discussions.* These questions are intended to reinforce the objectives for the weekly lesson. Please engage in thoughtful communication with your classmates and your professor. Answering that you agree or do not agree is not acceptable. You must discuss why. Further, an explanation of grading will be provided in the classroom.

*Cyber News Summary & Analysis.* Most weeks you will be required to write three summaries of cyber news stories. 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. Follow the directions posted each week. One of the most important things to remember is to not repeat a story covered by a previous respondent each week.

**Deadlines**

Distance learning gives you the flexibility to meet your professional, personal, and academic obligations. As a student, you are expected to follow the student course guidelines and submit your assignments on time. Late submissions will detract from your grade unless you have discussed the situation with me in advance and have an approved extension. Otherwise, late submissions will not be graded.

**Major Required Reading** (purchase or loan required)


NOTE: If there’s a package that includes both these items. Feel free to purchase that if it’s cheaper. You may also purchase access to the lab from the publisher – JBL.

Other readings and material will be placed in the lesson folders. Given the rapidly changing nature of this field, readings may change from those listed below. These will be announced.

**Course Requirements**

Current as of May 23, 2023
The following are the requirements for this course:

- **Discussion Boards**: Students will be evaluated on a) discussion board participation, b) news story analysis.
- **Laboratory Exercises**: The five required lab events are functionally pass/fail exercises (0 or 100 percent). Students will submit a final screenshot to confirm completion.
- **Mid-term Exam**: This will consist of multiple-choice, identification, and/or short essay questions. The mid-term will be given Week 4.
- **Final Exam**: This exam will include multiple choice, identification, and/or short essays. The exam will be completed in Week 7.
- **Extra Credit**: There may be opportunities for extra credit. Opportunities vary. Watch the classroom for opportunities. The primary means is via the “Bug Hunt” tool, which is simply a means of incentivizing students to report errors. This follows methods used in the greater cyber domain in which clients and white hat hackers are encouraged to report errors before they become a problem for the host.

### Evaluation Procedures

<table>
<thead>
<tr>
<th>Graded Instruments</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction (Week 1 – 50 points)</td>
<td>No Later Than (NLT) 11:55 p.m., Thursday w/ responses to others NLT 11:55 p.m. Sunday</td>
</tr>
<tr>
<td>Discussion Boards -- Weeks 1, 2, 3, 5, 6 (100 points/each)</td>
<td>NLT 11:55 p.m. Friday w/ responses to others by NLT 11:55 p.m. Sunday</td>
</tr>
<tr>
<td>News Analysis -- Weeks 2, 3, 5, 6 (100 points each)</td>
<td>News Analysis DBs – Due Weekly NLT 11:55 p.m. Sunday</td>
</tr>
<tr>
<td>Cyberwarfare Labs – Weeks 2,3,5,6,7 (100 points each)</td>
<td>Labs – Due Weekly NLT 11:55 p.m. Sunday</td>
</tr>
<tr>
<td>Cumulative Mid-Term Exam (350 points)</td>
<td>Week #4 NLT 11:55 p.m. Sunday</td>
</tr>
<tr>
<td>Cumulative Final Exam (400 points)</td>
<td>Week #7 NLT 11:55 p.m. Saturday</td>
</tr>
<tr>
<td>Extra Credit (TBD)</td>
<td>Bug Hunt, optional DBs, others TBD</td>
</tr>
<tr>
<td><strong>TOTAL (~2200 points)</strong></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Late submissions will not be graded.

### Reference Style

Current as of May 23, 2023
You may use any major academic reference styles: APA, MLA, APSA, Chicago, Turabian, etc. I prefer APA with parenthetical, in-line citations (Note: You’re likely to find some variations in the class, because I’m still converting the original courseware to the new class model). You may use any of these, but you should use it consistently. When grading, I mark down work that fails to use a consistent style. Pick one you like and stick with it.

**Grading Scale**

100 - 90 = A//89 - 80 = B//79 - 70 = C//69 – 60 = D // 59 - below = F

**Course Outline**

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Learning Objective</th>
<th>Readings (available in weekly lesson folders)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>History of Internet, Cybersecurity, &amp; Cyberwar</td>
<td>LO-3,4,5</td>
<td><strong>Wednesday - History of the internet</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• VIDEO: History of the internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• VIDEO: What does ICANN do</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Friday - History of cyber</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>REQUIRED PURCHASE OR RENTAL (Course Text)</strong> -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Chapple, Mike &amp; David Seidi. 2023. <em>Cyberwarfare: Information operations in a connected world</em>. Jones &amp; Bartlett Learning (Chap. 1 – Info as a military asset)</td>
</tr>
<tr>
<td>2</td>
<td>Internet Governance &amp; National Security</td>
<td>LO-1,2,3,4,5</td>
<td><strong>Monday – Targets &amp; Combatants</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Course text. Chap. 2 – Targets &amp; combatants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Wednesday - Internet Governance</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Course text. Chap. 3 – Cyber law &amp; ethics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Friday - Cybersecurity &amp; National Security</strong></td>
</tr>
</tbody>
</table>

Current as of May 23, 2023
<table>
<thead>
<tr>
<th>3</th>
<th>War in Cyberspace</th>
<th>LO-1,2,3,4,5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday – Evolving threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Skim: Memorandum for Chiefs of the Military Service Commanders of the Combatant Commands Directors of the Joint Staff Directorates - Subject: Joint terminology for cyberspace ops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schneider, Jacquelyn. 2018. “What war games tell us about the use cyber weapons in a crisis.”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Course text. Chap. 5 – “Evolving threat: From script kiddies to advanced attackers”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday - War in Cyberspace</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Course text. Chap. 6 – Social engineering &amp; cyberwarfare</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• VIDEO: Brantly, Aaron. 2015. “War in Cyberspace”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Deen, Thomas. 2020. “Russian expansion &amp; hybrid warfare”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friday - The Debate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Course text. Chap. 7 – “Weaponizing cyberspace”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rid, Thomas. 2012. “Cyber war will not take place”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Stone, John. 2013. “Cyber war will take place!”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schneider, Jacquelyn. 2018. “What war games tell us about the use of cyber weapons in a crisis.”</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>CAN &amp; CNE</th>
<th>LO-1,2,3,4,5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday – Outliers? Non-state actors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Course text. Chap. 8 – “Non-state actors in cyberwar”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bucci. Steven. 2012. “Joining cybercrime &amp; cyberterrorism: A likely scenario” in Chapter 4 of <em>Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday – CAN &amp; CNE Examples</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| • Farwell, James & Rafal Rohozinski. 2011. “Stuxnet and the...
| 5 | Cyber: Defense | Future of cyber war.
  - E-ISAC. 2016. Analysis of cyber attack on Ukrainian power grid:
  
  **Friday – Cryptography & Cyberwar**
  - Course text. Chap. 10 – “Cryptography & cyberwar”

| LO-1,2,3,4,5 | Monday – Defense I
  - Course text. Chap. 9 – “Defense-in-depth strategies”

|  | Wednesday – Defense II
  - Course text. Chap. 11 – “Defending endpoints”
  - Course text. Chap. 12 – “Defending networks”

|  | Friday – Defense III
  - Course text. Chap. 13 – “Defending data”

Current as of May 23, 2023
| 6 | Cyber War Issues | LO-1,2,3,4,5 | Monday – Military doctrine  
- Course text. Chap. 14 – “Cyberwarfare & military doctrine”  
- Dunlap, Charlie. 2021. ”Cyber actions and acts of war.”  

Wednesday – National security  

Friday - Human Rights  

| 7 | Cyberwar in the Future (FINAL EXAM) (COURSE EVALUATION) | LO-1,2,3,4,5 | Monday – Cyber Future  
- Course text. Chap. 15 – “Pandora’s Box: The future of cyberwarfare”  
- Ranger, Steve. 2017. “Now that cyberwarfare is out of the shadows.”  
- Other readings TBD  

**Academic Services**  
The [Online Library Resource Center](#) is available to enrolled students from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources generally not available through search engines on the open Web. In addition, the
Center provides access to special learning resources, which the University has contracted to assist with your studies. Questions may be directed to libraryref@utep.edu.

- **Library and Inter Library Loan:** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.

- **Electronic Books:** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.

- **Electronic Journals:** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.

- **Turnitin** is a tool to improve student research skills that also detect plagiarism. Turnitin.com provides resources on developing topics and assignments that encourage and guide students in producing papers that are intellectually honest, original in thought, and clear in expression. This tool helps ensure a culture of adherence to the University's standards for intellectual honesty. Turnitin.com also reviews students' papers for matches with Internet materials and with thousands of student papers in its database and returns an originality report to instructors and/or students.

For the INSS Library Guide, please go to: http://libguides.utep.edu/inss
Email: Angela Lucero, INSS Librarian ajmartinez5@utep.edu

**Tutoring and Writing Services**

The University Writing Center (UWC) provides comprehensive resources for all students, faculty, and the community when it comes to writing. For students, this includes face-to-face and online writing consultations--from freshman to doctoral students.

The UWC can help you with the following writing issues:

- Analyze your audience
- Understand the different types, or genres, of writing
- Decide on the appropriate form and style for your writing
- Brainstorm ideas and assist you organize your thoughts
- Find the right words to express yourself
- Decide on the best ways to pre-write, write, and revise your drafts
- Manage your grammar and mechanical issues
- Assist with word processing software
- Provide instruction on documenting and citing your sources

You may visit them in Library 227 via live, online consultations. For best results, consult with them early and often.

Another excellent resource is Purdue University’s Online Writing Lab. This is especially helpful in sorting out reference style and construction issues.

**Disability Statement**

As per Section 504 of the Vocational Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) of 1990, if a student needs an accommodation then the Office of Disabled Student Services located at UTEP need to be contacted. If you have a condition, which may affect your ability to perform successfully in this course, you are encouraged to discuss this in confidence with the instructor and/or the director of the Disabled Student Services. You may
call 915-747-5148 for general information about the American with Disabilities Act (ADA) and the rights that you have as a UTEP student with a disability.

Individuals with disabilities have the right to equal access and opportunity. It is the student's responsibility to contact the instructor and Center for Accommodations and Support Services offices at The University of Texas at El Paso.

Technical Requirements
The University of Texas at El Paso provides free 24/7 Helpdesk support to academic students and faculty members teaching on-line through the Help Desk. The Helpdesk can provide answers to questions about using technology and services, as well as technical support. Please visit the technical support page for more information.

Microsoft Office. If you do not have Microsoft Office, check with your University of Texas branch store for the special Microsoft Office package that includes Word, Excel, and PowerPoint.

Contact the UTEP Bookstore at (915) 747-5594 for more info. Adobe Flash: This application is for advanced multimedia presentations/interactions over the internet. You may download this player from the Adobe Download site.

Netiquette
We seek to promote the advance of knowledge through positive and constructive debate. Debate does not include descent to personal attacks or attempts to stifle the discussion of others. Engage the ideas without attacking the person or blocking topics.

Academic Integrity and Plagiarism
Academic dishonesty is prohibited. This includes cheating, collusion, and plagiarism. The UTEP Handbook of Operating Procedures provides more details on these items, however, to put it most simply, if you're taking someone else's work and using it as your own it's wrong. This includes copying from a friend, using material from sources without attribution, and misuse or stealing of tests or other graded instruments. Any act of academic dishonesty is unacceptable and will not be tolerated. Violations will be referred to the Dean of Students Office for possible disciplinary action.

Disclaimer Statement
Course content may vary from the outline to meet the needs of specific classes, at the discretion of the instructor.

Copyright 2023 © Dr. Brett Morris & The University of Texas at El Paso