ITMS 557 Introduction to Cyber Warfare
Course Syllabus

Faculty Information
Professor: Louis F. McHugh IV
Office: Wheaton, IL (Rice Campus)
Telephone: (630) 682-6040
Email: lmchugh@iit.edu (preferred method of contact)
Office Hours: By Appointment via louismchugh.youcanbook.me
Online Hours: via Skype by Appointment

Course Description
Cyber warfare is defined as “warfare waged in cyberspace,” which can include defending information and computer networks, deterring information attacks, as well as denying an adversary’s ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield. Students participating in this discussion-based course will explore the current state of cyber security from national and international perspectives, and consider cyber-based operations through the lens of a government pursuing strategic goals. How might their actions impact industry ability to conduct business operations? What does the current threat environment look like? The course will include extensive discussions and student presentations.

Prerequisites: There are no specific prerequisite courses.

Credits: 3-0-3
Lecture Day, Time, and Location: TBD

Course Objectives
• Describe cyber warfare and cyber security concepts.
• Discuss the cyber threat landscape, or “threatscape.”
• Recall the types of threats (attackers) that exist, as well as the types of potential and historical targets.
• Explain the impact the cyber domain has on conventional military strategy.
• Describe planning considerations involved with cyber warfare.
• Identify overarching principles of strategic warfare and instruments of national power.
• Identify doctrine concepts and explain how they relate to strategic warfare.
• Recall U.S. cyber doctrine principles and describe how they fit into the larger picture of strategic warfare and instruments of national power.
• Describe internationally varying approaches to cyber warfare.
• Identify, describe, and employ tools used in cyber-attacks from offensive and defensive postures.
• Recall and explain cyber espionage concepts.
• Describe state-sponsored espionage capabilities and targets.
• Identify and describe examples of large-scale cyber espionage and data exfiltration.
• Identify and describe offensive tactics and procedures used in cyberspace.
• Define Cyber Crime and describe what is it and how it affects the overall world economy as well as individuals.
• Discuss where we go from here: What will Cyber look like in a month, a year, and 5 years from now? What will potential policies look like as we attempt to define this problem globally?
Course Outcomes

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

• Describe cyber space as the fifth domain of war.
• Explain how current cyber doctrine affects a nation's use of its instruments of national power, the status of current national and international cyber-related policies, and the impact those policies and doctrine may have on private business.
• Describe the relationship between our global economy, cybercrime and espionage.
• Apply this knowledge to define policy as well as operational, technical, and managerial controls in a wide variety of settings, including the corporate space, government, defense, law enforcement, and intelligence.
• Employ basic cyber warfare methodologies in offensive and defensive postures.

Student Responsibilities

Do your reading, show up to class, and participate! This is a discussion-based class, so your thoughtful participation is essential. Get your readings done early, look up subjects you find interesting or have questions about, and come to class reading to share your ideas. Lastly, make sure your assignments, presentation, and final exam reflect your best work. There aren't many graded items in this course, so each of them are important.

Readings

Readings for the class will be assigned from the textbook as well as in the form of handouts and online reading. It is essential that you do all readings before coming to class on the assigned date. Additionally, each week all students are required to come to class with at least two prepared “discussion topics.” These discussion topics should be based on material covered in the reading. The point is for you to identify at least two things from the reading you find interesting, want to discuss, or have thought-provoking questions about. Note these items down and be prepared to share them in class. This will be included in your class participation grade.

The readings are an integral part of the class and will form the basis for any class discussion on the topic. Online resources will be linked from Blackboard or will be posted on Blackboard.

Assignments

Assignments will be made on a week-by-week basis. All assignments will be submitted via Blackboard. An assignment will usually be due on or before the class meeting date one week following the date that it was assigned.

Academic Honesty Policies

Any violations of IIT policies regarding academic honesty and or integrity will be referred automatically to the appropriate college authorities for disposition. Please see appropriate pages in the IIT and ITM Student Handbooks for definitions and regulations. Any academic dishonesty (cheating) will result in either (1) a zero (0) for the assignment, program, test, quiz or exam, or (2) a failing grade for the course, depending on the severity of the dishonesty. Bottom-line: do not do it.

Examples of academic dishonesty include, but are not limited to, the following:

• Representing the work of others as your own.
• Obtaining or using unauthorized tests or quizzes.
• Use of unauthorized material, such as notes or books, during an examination.
ITMS 557  Introduction to Cyber Warfare  

Course Syllabus

- Open cheating during an examination, such as looking at another student’s examination.
- Receiving or giving unauthorized assistance from/to other students.
- Revision of graded work in an effort to obtain additional credit.

Withdrawal Policy
Non-attendance does not constitute withdrawal from the course. You must formally drop or withdraw from the course per the applicable university Bulletin. Student not attending the course as of the midterm will receive a grade of NA and are expected to withdraw from the course, or they will receive a failing grade for the course at the end of the semester.

Incomplete Policy
Incomplete grades are generally not given without sound reason and documented evidence as described in the IIT Student Handbook. In all cases, for a student to receive an incomplete, he or she must be passing and must have completed a significant portion of the course. If an incomplete grade is given, the student must complete all work by the date agreed upon by them and the instructor.

Classroom behavior
During the class time, considerate conduct by all persons is important to a favorable learning environment. Any infringement on the rights of others to get an education will be dealt with in an appropriate manner. Please set all electronic devices such as cell phones or pages to silent modes. Do not let you phone go off in the class. If you need to leave early, or miss a class, make every effort to see me in advance!

Grading Criteria

<table>
<thead>
<tr>
<th>Grading Criteria</th>
<th>Graduate Student Grading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments ...........30%</td>
<td>A ................ 90% and above</td>
</tr>
<tr>
<td>Class Participation ...10%</td>
<td>B ................. 80% to &lt;90%</td>
</tr>
<tr>
<td>Presentation ..........30%</td>
<td>C ................ 65% to &lt;80%</td>
</tr>
<tr>
<td>Final Exam .............30%</td>
<td>E ................ Below 65%</td>
</tr>
</tbody>
</table>

ADA Statement
Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312 567.5744 or disabilities@iit.edu.
Required Books

**Paperback:** 164 pages  
**Publisher:** Syngress; 1 edition (November 30, 2012)  
**ISBN-10:** 0124047378  
**ISBN-13:** 978-0124047372

Purchase as ebook:  
- [https://play.google.com/store/books/details?id=ARTp9HoCsp4C](https://play.google.com/store/books/details?id=ARTp9HoCsp4C)


**Paperback:** 336 pages  
**Publisher:** Syngress; 1 edition (June 18, 2013)  
**ISBN-10:** 0124078141  
**ISBN-13:** 978-0124078147

Purchase as ebook:  
- [https://www.academia.edu/2320964/Introduction_to_Cyber-Warfare_A_Multidisciplinary_Approach](https://www.academia.edu/2320964/Introduction_to_Cyber-Warfare_A_Multidisciplinary_Approach)  
- [https://play.google.com/store/books/details?id=ziq8LPWfgkIC](https://play.google.com/store/books/details?id=ziq8LPWfgkIC)
## Course Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Week</th>
<th>Topic</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Course requirements</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| 2    | Cyber warfare “threatscape” |  | The Basics of Cyber Warfare, pages xiii-14  
2014 Data Breach Investigations Report, pages 1-12  
Transforming Cybersecurity, pages 1-5  
Joint Publication 1, pages I-2 – I-8 |
| 3    | Operations |  | The Basics of Cyber Warfare, pages 15-28  
Joint Publication 1, pages I-3  
Joint Publication 5, figures III-5 & III-10 |
| 4    | Doctrine |  | The Basics of Cyber Warfare, pages 31-49  
The Enemy as a System, pages 1-13  
Joint Publication 1, pages I-11 – I-16 |
| 5    | Case Studies |  | To be given out upon assignment |
| 6    | TTPs and Tools, part 1 |  | The Basics of Cyber Warfare, pages 51-66  
Pacemakers and Implantable Cardiac Defibrillators  
FBI worried as DOD sold counterfeit Cisco gear.  
Introduction to cyber-warfare a multidisciplinary approach, Chapter 13 |
| 7    | TTPs and Tools, part 2 |  | The Basics of Cyber Warfare, pages 51-66  
Pacemakers and Implantable Cardiac Defibrillators  
FBI worried as DOD sold counterfeit Cisco gear.  
Introduction to cyber-warfare a multidisciplinary approach, Chapter 13 |
| 8    | Espionage |  | Introduction to Cyber-Warfare, pages 113-132  
2014 Data Breach Investigations Report, pages 38-42  
Intel Prep of the Cyber Environment, pages 140-143 |
| 9    | Offense |  | Introduction to Cyber-Warfare, Chapter 5  
Introduction to cyber-warfare a multidisciplinary approach, Chapter 3 |
| 10   | Defense |  | Introduction to Cyber-Warfare, Pages 99-112  
“U.S. Cyber Command Fact Sheet, pages 1-3  
Office of Cybersecurity and Communications, mission statement  
“The Comprehensive National Cybersecurity Initiative.” |
| 11   | Cyber Crime |  | Introduction to cyber-warfare a multidisciplinary approach, Chapter 7 & 8  
Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers |
| 12   | Way Ahead |  | Introduction to Cyber-Warfare, Chapter 8 & 9  
The Military Role in National Cybersecurity Governance |
| 13   | Presentations | N/A | |
| 14   | Presentations | N/A | |
| 15   | Presentations | N/A | |
| 16   | Final exam due | N/A | |
Attachment 1 – Presentation Guidelines

“One who forms a judgment on any point, but cannot explain himself clearly to the people, might as well never have thought at all on the subject.”
-Pericles, ~500 B.C.

Requirements
• Deliver a 15-20 minute presentation on a cyber-warfare-related topic of your choice.
• The topic must be well-defined. For example, “Cyber Warfare Defense” is too broad. Instead, choose something like “The Challenges of Implementing DHS’s Einstein 3 Program.”

Grading Rubric
A: 25 – 30 points
B: 19 – 24 points
C: 13 – 18 points
F: < 13 points

<table>
<thead>
<tr>
<th>Element</th>
<th>Excellent</th>
<th>Good</th>
<th>Adequate</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eye contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vocal variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Body language (including appearance and gestures)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time requirements met</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear thesis and purpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organized body with main points</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Effective use of visual aids</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good research and supporting material</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conclusion</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did you maintain appropriate eye contact?</td>
</tr>
<tr>
<td>Varied pitch and delivery, were you appropriately expressive?</td>
</tr>
<tr>
<td>Were you gestures purposeful? Did you avoid nervous mannerisms?</td>
</tr>
<tr>
<td>Did you complete your presentation within the allotted time?</td>
</tr>
<tr>
<td>Did you introduce yourself? Did you gain the audience’s attention?</td>
</tr>
<tr>
<td>What are you presenting? Why should I care?</td>
</tr>
<tr>
<td>Was your presentation well organized? Can I recall your main points?</td>
</tr>
<tr>
<td>Were your visual aids clear and useful?</td>
</tr>
<tr>
<td>Was your supporting material effective and impactful? Was there enough?</td>
</tr>
<tr>
<td>Did you effectively summarize your main theme?</td>
</tr>
</tbody>
</table>
Attachment 2 – Current Event Assignment Guidelines

Requirements

- All students will complete two five-minute briefings on current cyber-warfare-related news events.
  - Avoid excessively technical events unless you can tie it into broader concepts that impact a wide audience.

- Your current event briefing should include a summary of the event that covers the five W's (who, what, when, where and why), as well as some thoughtful analysis. Some questions to consider in your analysis include:
  - Why does this matter?
  - Who might it impact?
  - Are there any important historical considerations that might help improve our understanding of what’s happening?

- Come prepared on your assigned day with a primary and secondary current event in case an earlier presenter has the same story you do. Have a copy ready for reference to help answer questions other students may have.

- These are pass/fail assignments.

Recommended News Sources that Specialize in Cyber Security

- www.scmagazine.com
- www.darkreading.com
- www.krebsonsecurity.com
- www.arstechnica.com/security/
- www.securityfocus.com
- www.slashdot.org/stories/security
- www.secureworks.com/resources/blog/research/
- www.fierceitsecurity.com
- www.jinfowar.com
- And many others can be found here: http://www.itm.iit.edu/resources/itsecurity.php