Macintosh HD:Users:ers:Dropbox:ACTIVE:JHU-logos:WSE:small:PDF:whiting.small.horizontal.black.pdf

**Syllabus**

**EN.650.681 Global Cybersecurity**

**Global Cybersecurity Trends and Practices**

**Fall, 2018**

**(3 credits, EQ)**

**Description**

This course provides an overview of cybersecurity capabilities and trends in the global community, complementing knowledge gained in other courses. International organizations engaged in cybersecurity and the national strategies of many countries are examined in detail. Students will gain insights into the political, economic, military, and technological components of cybersecurity as practiced in the U.S., UK, China, Russia, and other countries. The course is designed around four general themes: global cyber threats, strategies and policies in response to cyber threats, comparative cybersecurity capabilities of nation-states; and cybersecurity in international politics. Students will also gain an appreciation of how key cybersecurity issues like critical infrastructure protection and information sharing are addressed in an international context. Extensive reading is required from sources that will be available on Blackboard, on-line, or via the JHU Library’s electronic reserves.

**Prerequisites**

Recommended: Introduction to Information Security (650.401/601)

**Instructor**

Dr Terry Thompson (tthomp83@jhu.edu; tlthomp@aol.com)

Office: Malone 363

Office hours: Tuesday and Thursday, 3:00-4:00 pm and by appointment

**Class Meetings**

4:30-5:45, Tuesday and Thursday

Olin 305

**Textbook**

*Fatal System Error* by Joseph Menn is required for the book review assignment. Students may purchase this book online or at the university bookstore. All other reading assignments will be provided on Blackboard (see below under “Assignments and Readings.”)

**Course Objectives**

By the completion of this course, students should be able to:

1. Describe the major trends in the global cyber threat environment
2. Identify the missions, authorities, and responsibilities of key international cybersecurity organizations
3. Describe the complexities in the global cybersecurity environment
4. Compare cybersecurity strategies and approaches of various nations
5. Identify emerging international trends in offensive and defensive cybersecurity practices
6. Describe the challenges to the U.S. presented by the global cybersecurity environment

**Course Topics**

* Global cyber threats, vulnerabilities, and data breaches
* Global cybersecurity concepts (e.g. strategies, governance, evaluation frameworks)
* Organizations engaged in global cybersecurity
* Comparative national cybersecurity strategies and initiatives
* Critical infrastructure protection and risk assessments in an international context
* International and regional cybersecurity strategies and agreements
* Cybersecurity standards and how they are applied to risk management
* Global trends in data protection
* Use the internet as a tool for political control
* Cybercrime statistics, trends, modalities, and law enforcement response
* Cyber espionage practitioners and tactics, techniques and procedures
* Cyber war and deterrence
* Problems and prospects for global cybersecurity collaboration

**Course Expectations & Grading**

The course will consist of lecture and classroom discussions supplemented by individual and team research. Students will be expected to have read all assigned readings for each class and engage actively in classroom discussions. Students will also conduct individual and group research on relevant topics and present their findings to the class in oral presentations. Homework, quizzes and a mid-term exam are required. Written assignments include homework, the midterm exam, and a book review. In addition, each student will provide an oral presentation on a current event in global cybersecurity and participate in a team research project culminating in a presentation to the class.

**Grading Criteria**

**Course work Grade distribution**

Current Events Presentation and Homework 20%

Quizzes 20%

Midterm Examination 20%

Book Review 15%

Research Project and Presentation 25%

* Note: Additional information and grading rubrics will be provided for the mid-term, book review, and research project assignments.

Assignment grades and final grades will be determined as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 100-98% | A+ | 89-87% | B+ | 79-70% | C |
| 97-94% | A | 86-83% | B | 60-69% | D |
| 93-90% | A- | 82-80 | B- | <59% | F |

**Assignments & Reading**

Extensive literature is available about international and national cybersecurity. The best and most current material is not yet in textbook format. For this reason, all readings will be posted on the course Blackboard site except for *Fatal System Error* by Joseph Menn, which we will use for the book review. This book is available on line; the JHU bookstore may have a few copies as well.

To locate the reading assignments for each class, look in the **Course Content** section of the course Blackboard site. In the folder “**Reading Assignments**,” you will find readings for each class based on the topic for that class. For example, assigned reading for the first class is listed under “Global Cyber Threats and Vulnerabilities,” which is the topic for the class on 4 September. Additional readings may be assigned during the course.

**Graded Assignments**

1. **Class participation** is an important aspect of this course and will be graded based on satisfactory completion of the current events presentation and homework assignments.
   1. **Current Events Presentations:** Maintaining awareness of the dynamic global cybersecurity environment is an important component of this course. For this reason, each student will do a brief, 10-minute presentation to the class on a current topic or event related to global cybersecurity. Media resources may be used but are not required. The most successful presentations will:
      * Quickly identify the essential information about the topic or issue and the relevance to the course
      * Organize information clearly and concisely
      * Identify the source of information and an assessment of the validity of the source.

**Homework**: Three short (1-2 pages each) homework assignments will be assigned to focus on the assigned reading materials and to prepare for class discussions.

1. **Quizzes**: Two quizzes are required in the course. The purpose of the quizzes is to reinforce learning from the class lectures and reading assignments.
2. **Midterm Exam:** The midterm will be a take-home exam covering material addressed in the first part of the course. Students will write brief essays in response to assigned questions. A grading rubric will be provided for this assignment.
3. **Book Review**: Students will write a review of *Fatal System Error* by Joseph Menn. The review should be 1000-1250 words in length and should provide analysis about the significance of the book in the context of global cybercrime. Additional information about this assignment will be provided in class. A grading rubric will be provided for this assignment.
4. **Research Project and Presentation**: Research projects will focus on the intersection of cybersecurity technology and strategy or policy in the international environment. These may be original projects that focus on regional or national strategies and their technology implications, or another aspect of global cybersecurity. Topics must be approved by the professor. Research projects will be conducted by small teams. Teams will present the results of their research to the class in an oral presentation accompanied by a written abstract of the project and bibliography. Presentations will be scheduled during the last weeks of the course. A grading rubric will be provided for this assignment.

**Global Cybersecurity Trends and Practices**

**Class Schedule – Fall 2018**

**Note: Reading assignments for each class are available on Blackboard.**

|  |  |
| --- | --- |
| **Date** | **Topic** |
| 9/4 | **Introductions and Course Overview**   * Syllabus review, assignments, course expectations |
| 9/6 | **Global Cyber Threats and Vulnerabilities**   * Lecture and discussion; Major threats in global environment, targets of attacks, threat actors, tradecraft, and impacts |
| 9/11 | **Global Cyber Threats: Attack Surfaces and Attack Vectors**   * What are the major vulnerabilities hackers use and how do they exploit them? * DRAGONFLY and other recent attacks * ***Assignment: Homework 1 - Case studies of global cyber threats (Due 9/13)*** |
| 9/13 | **Foundations of Global Cybersecurity**   * Lecture: Role of the United Nations in the development and use of the Internet * Discussion: Case studies of global cyber threats (Homework 1) |
| 9/18 | **Global Governance of the Internet**   * Lecture: Technology stability amidst political turmoil; organizations and issues in global cybersecurity governance * Discussion: The Internet and net neutrality * ***Quiz 1: Global cybersecurity organizations, governance and issues (Due 9/23)*** |
| 9/20 | **Cybersecurity Strategies and Frameworks**   * Lecture: ITU, ENISA, NATO and national strategies * Discussion: Comparison of strategy frameworks |
| 9/25 | **National Cybersecurity Strategies**   * Lecture: The U.S. National Cybersecurity Strategy * ***Assignment: Homework 2 – Summarize a national cybersecurity strategy and compare it to the ITU framework (Due 9/27)*** |
| 9/27 | **Regional and International Organizations and Strategies**   * Lecture: Regional and international organizations and their role in cybersecurity * Discussion: Cybersecurity strategies of select countries(Homework 2) |
| 10/2 | **Critical Infrastructure Protection Background and History**   * Lecture: Marsh Commission and U.S. approach; European approach * Discussion: Book review assignment and research tips for team projects |
| 10/4 | **Critical Infrastructure Protection (CIP) Implementation**   * Lecture: U.S. National Infrastructure Protection Plan (NIPP) * Discussion: CIP plans of select countries * ***Quiz 2: Cybersecurity strategy and critical infrastructure protection (Due 10/7)*** |
| 10/9 | **International Cybersecurity Standards**   * Lecture: ISO/IEC, NIST Cybersecurity Framework * Discussion: Why are cybersecurity standards important? |
| 10/11 | **Cybersecurity Risk Management**   * Lecture: Applying NIST Cybersecurity Framework (CSF) to risk management * Discussion: NIST CSF categories (control groups) * ***Assignment: Homework 3 - Assess one category (control group) of the NIST Cybersecurity Framework (Due 10/15)*** |
| **Date** | **Topic** |
| 10/16 | **Data and Data Protection**   * Lecture and discussion: Global concerns about data protection; data localization * Discussion: NIST categories (control groups) (Homework 3) |
| 10/18 | **Privacy, Surveillance, and Control**   * Lecture and discussion: U.S. and international context for privacy; internet freedom and information/content controls |
| 10/23 | **Cybercrime**   * Lecture: Cybercrime trends and impacts; law enforcement response * Discussion: *Fatal System Error* |
| 10/25 | **Research Project Updates**   * Assignment: Each team to provide a 10-15 minute update on their research projects. |
| 10/30 | **National Cybersecurity Policies and Programs**   * Lecture and discussion: The U.S. and UK * ***Assignment: Book reviews due*** |
| 11/1 | ***Midterm Exam Available (Due 11/5)*** |
| 11/6 | **National Cybersecurity Policies and Programs**   * Lecture and discussion: China |
| 11/8 | **National cybersecurity Policies and Programs**   * Lecture and discussion: Russia |
| 11/13 | **Cyber espionage**   * Lecture and Discussion: Threat actors, motivations, tradecraft |
| 11/15 | **Cyber war and deterrence**   * Lecture and discussion: Threat actors, motivations, tradecraft, impacts |
| 11/20  11/22 | **Thanksgiving break – No class** |
| 11/27 | **Global Cooperation on Cybersecurity: Problems and Prospects**   * Lecture: Global Cooperation on Cybersecurity * **Assignment: Research Project Presentations** |
| 11/29 | * **Assignment: Research Project Presentations** |
| 12/4 | * **Assignment: Research Project Presentations** |
| 12/6 | **Course Summary and Wrap-up**   * Assignment: Extra time if needed for research project presentations |

**Ethics**

The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful, abiding by the *Computer Science Academic Integrity Policy*:

Cheating is wrong. Cheating hurts our community by undermining academic integrity, creating mistrust, and fostering unfair competition. The university will punish cheaters with failure on an assignment, failure in a course, permanent transcript notation, suspension, and/or expulsion. Offenses may be reported to medical, law or other professional or graduate schools when a cheater applies.

Violations can include cheating on exams, plagiarism, reuse of assignments without permission, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition. Ignorance of these rules is not an excuse.

Academic honesty is required in all work you submit to be graded. Except where the instructor specifies group work, you must solve all homework and programming assignments without the help of others. For example, you must not look at anyone else’s solutions (including program code) to your homework problems. However, you may discuss assignment specifications (not solutions) with others to be sure you understand what is required by the assignment.

If your instructor permits using fragments of source code from outside sources, such as your textbook or on-line resources, you must properly cite the source. Not citing it constitutes plagiarism. Similarly, your group projects must list everyone who participated.

Falsifying program output or results is prohibited.

Your instructor is free to override parts of this policy for particular assignments. To protect yourself: (1) Ask the instructor if you are not sure what is permissible. (2) Seek help from the instructor, TA or CAs, as you are always encouraged to do, rather than from other students. (3) Cite any questionable sources of help you may have received.

On every exam, you will sign the following pledge: "I agree to complete this exam without unauthorized assistance from any person, materials or device. [Signed and dated]". Your course instructors will let you know where to find copies of old exams, if they are available.

You can find more information about university misconduct policies at these sites:

* For undergraduates: <http://e-catalog.jhu.edu/undergrad-students/student-life-policies/>
* For graduate students: <http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/>

**Students with Disabilities**

Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516-4720, [studentdisabilityservices@jhu.edu](mailto:studentdisabilityservices@jhu.edu) .