Course Syllabus

IDC 5602 - Cybersecurity: A Multidisciplinary Approach
(M/W sections)

School of Modeling, Simulation, and Training (SMST)

3.0 Credit Hours

Table of Contents

IMPORTANT: All of the above are required items in the course syllabus and link to the appropriate headings below. If you change these links or the associated headings below, the Table of Contents may need to be re-coded. If you notice the links are not working, email Webcourses@ucf.edu.

Instructor Information

- Instructors: Sean Mondesire, Ph.D.
- Office Location: Webcourses
- Office Hours: By appointment
- Digital Contact: Webcourses@UCF messaging

Teaching Assistants

- Teaching Assistant: Malic Dekkar
- Email: Webcourses@UCF messaging

Course Information

- Term: Fall Term, 2022
- Course Number & Section: IDC 5602, M/W sections
- Course Name: Cybersecurity: A Multidisciplinary Approach
- Credit Hours: 3.0 Credit Hours
- Class Meeting Day: Wednesdays
- Class Meeting Time: 5pm
- Class Location: **Online (W) and Room 233, P3 (M)**
- Course Modality: W, M

Enrollment Requirements

Course Prerequisites (if applicable): N/A
Course Co-requisites (if applicable): N/A
Other Enrollment Requirements (if applicable): N/A

Course Description

This is a core course for the Graduate Certificate in Modeling and Simulation of Behavioral Cybersecurity.

Purpose: To expand the student's understanding of the principles of cybersecurity, to include the behavioral aspects of cyber. Most advanced education courses in cyber consist of technical aspects - i.e., learning how to program and use those programs and scripts to defend against modern hackers. This course looks beyond the "1s and 0s" and considers the cognitive tools needs for the cyber fight.

IDC 5602 consists of modeling and simulation fundamentals as applied to cybersecurity including operating system installation and administration for hardware, network architectures, layers, protocols, and configurations. Cyber threats and vulnerabilities are discussed, as well as the behavioral aspects to cybersecurity. Valid cyber training and education models are explored. Modeling and simulation concepts are discussed as complements to activities supporting cybersecurity in small and large organizations.

More info on the graduate certificate
- http://www.graduatecatalog.ucf.edu/programs/program.aspx?id=11981Links to an external site.. This certificate provides students with an interdisciplinary modeling and simulation approach to cybersecurity with a particular emphasis on the behavioral aspects of cybersecurity and cyber operations. It is beneficial to individuals who have an

interest in interdisciplinary studies and problem solving for modeling, simulation, and behavioral aspects of cybersecurity.

Course Materials and Resources

Required Materials/Resources

- No mandatory textbook. But, I recommend that the students buy the textbook (Hacker Techniques, Tools, And Incident Handling / Edition 2 by Sean-Philip Oriyano) now for the follow-on, Spring 2020 Cyber Operations Lab (CNT 5410L): http://www.barnesandnoble.com/w/hacker-techniques-tools-and-incident-handling-sean-philip-oriyano/1118725907?ean=9781284031713&itm=1&usri=9781284031713 (Links to an external site.). This text contains good background information for some of the coursework in this intro IDC 5602 course.
- Further, the rest of the material that will be used for this class will mainly consist of academic and military texts and information sources:
    - DOD Cyber Strategy, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Links to an external site.)DOD Cyber Strategy (Links to an external site.)
    - DOD Cyber Strategy: (Links to an external site.)Federal Bureau of Investigation's Cyber Crime Info Page, https://www.fbi.gov/about-us/investigate/cyber (Links to an external site.)
    - Joint Publication 3-12, “Cyberspace Operations,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (Links to an external site.)

Optional Materials/Resources

- United States Computer Emergency Readiness Team (US-CERT), https://www.us-cert.gov (Links to an external site.)
- SANS Reading Room, http://www.sans.org/reading-room/ (Links to an external site.)
- US Army Cyber Center of Excellence, Fort Gordon, GA, http://cybercoe.army.mil (Links to an external site.)
- DARPA Cyber Grand Challenge, https://cgc.darpa.mil (Links to an external site.)
- Department of Homeland Security, Cybersecurity, http://www.dhs.gov/topic/cybersecurity (Links to an external site.)
- SANS @RISK Newsletters, http://www.sans.org/newsletters/at-risk/xv/23 (Links to an external site.)

- Oak Ridge Cyber Analytics, http://orca.ornl.gov/Oak_Ridge_Cyber_Analytics.html (Links to an external site.)
- Institute for Simulation and Training, http://www.ist.ucf.eduLinks to an external site.
- Society for Computer Simulation, http://www.scs.org (Links to an external site.)
- U.S. Army PEO STRI "Program Element Office, Simulation, Training and Instrumentation", http://www.peostri.army.mil/ (Links to an external site.)
- RDECOM, "US Army Research, Development and Engineering Command", http://www.army.mil/rdecom/ (Links to an external site.)
- U.S. Air Force Agency for Modeling and Simulation, http://www.afams.af.mil/ (Links to an external site.)

Third-Party Accessibility and Privacy Statements

N/A

Student Learning Outcomes

- Students will be able to create cybersecurity policies and procedures to help secure a medium-sized organization's information technology infrastructure.
- Students will understand the latest techniques hackers employ to test out cyber defenses.
- Students will analyze the mission and strategy of the U.S. government agencies who protect our portion of the Internet.
- Students will discuss hypothetical issues of cyber security with other students in the group Discussions format.

Course Activities

- **Short Bio (2 points)**

Post a short description of your background (under "Discussions"), what you expect to get out of this course, your current and past professional experience, and maybe something interesting about you. You might also post a picture of yourself.

- **Assignments (50 points)**

Three written assignments will be on specific issues related to topics covered in the course.

- **Discussions (28 points)**

Discussion questions will be released according to the class scheduled as specified in this Syllabus, and will be available for posting the Monday of the first week and close the Friday of the following week. During this period you need to make a minimum of three postings, the first of which should be about one or two paragraphs and written to be the first posting in a thread of discussion. Second and subsequent postings could be responses to someone else's initial posting. Use full reference citations as appropriate. Discussion forums, once open will remain open until the end of class and you may want to carry on a discussion, after the grading period ends.

Use the following conventions when composing a discussion posting:

1. During a Discussion assignment, deadlines for posting to and replying will be specified with each assignment. It is a good practice to always check the Discussions folder multiple times during the week.
2. If you want to send a personal message to the instructor or to another student, use e-mail rather than the discussions.
3. Use the appropriate discussion topic; don't post everything on the "Main" discussion topic.
4. A helpful hint for use with both discussions and e-mail - compose your message in your word-processing application in order to check spelling, punctuation, and grammar - then copy and paste your composition into e-mail or the discussion. This also saves online time.
5. Everyone should feel free to participate in class and online discussions. Regular and meaningful discussion postings constitute a substantial portion of your grade.
6. Be courteous and considerate. It is important to be honest and to express yourself freely, but being considerate of others is just as important and expected online, as it is in the classroom.
7. Explore disagreements and support assertions with data and evidence.
8. "Subject" headings: use something that is descriptive and refer to a particular assignment or discussion topic when applicable. Some assignments will specify the subject heading.
9. Use the "reply" button rather than the "compose" button if you are replying to someone else's posting.
10. Do not use postings such as "I agree," "I don't know either," "Who cares," or "ditto." They do not add to the discussion, take up space on the Discussions, and will not be counted for assignment credit.
11. Avoid posting large blocks of text. If you must, break them into paragraphs and use a space between paragraphs.

- **Out-of-class Final (20 points)**

This take-home final exam consists of a series of questions relating to course content not covered in the weekly assignments.

** Late assignments will receive a 10% deduction per day late. Assignments more than 2 days late are not accepted; this excludes the Final Exam, which will not be accepted late at all.*

Activity Submissions

Please submit all work via webcourses. If you need any assistance contact me or the GTA via webcourses mail immediately!

Attendance/Participation

This is a graduate level class. Attendance will not be taken but all work must be completed on time. Check webcourses frequently!!

Make-up Exams and Assignments

Per university policy, you are allowed to submit make-up work (or an equivalent, alternate assignment) for authorized university-sponsored activities, religious observances, or legal obligations (such as jury duty). If this participation conflicts with your course assignments, I will offer a reasonable opportunity for you to complete missed assignments and/or exams. The make-up assignment and grading scale will be equivalent to the missed assignment and its grading scale. In the case of an authorized university activity, it is your responsibility to show me a signed copy of the Program Verification Form for which you will be absent, prior to the class in which the absence occurs. In any of these cases, please contact me ahead of time to notify me of upcoming needs.

Assessment and Grading Procedures

Assignment	Percentage of Grade
Short Bio	2%
Assignment 1	10%
Assignment 2	20%
Assignment 3	20%
Discussions (4 each)	28% (7% each)
Final Exam	20%

Total	100%

Letter Grade	Points
A	93 – 100 points
A-	90 – 92 points
B+	87 – 89 points
B	83 – 86 points
B-	80 – 82 points
C+	77 – 79 points
C	73 – 76 points
C-	70 – 72 points
D+	67 – 69 points
D	63 – 66 points
D-	60 – 62 points
F	59 and below

Consult the latest Undergraduate or Graduate catalog. for regulations and procedures regarding grading such as Incomplete grades, grade changes, and grade forgiveness.