

I. Course Information

- Course Title: *IDC 6600 - Emerging Cyber Issues*
- Credit Hours: 3.0
- Semester/Year: Summer 2023, Session "C"
- Location: Lectures will be held online for both "M" and "W" sections each Tue in the Summer "C" term from 3pm to 5:50pm. Lectures are recorded each week in Zoom.

Instructors: Dr. Bruce Caulkins and Dr. Sean Mondesire

- **Office Hours:** By appointment.
 - **Email:** Use Webcourses Inbox.
-

II. Course Goals and Description

Goals: By the end of this course, our students will:

- Explore interdisciplinary issues for conducting research in behavioral aspects of cybersecurity
- Understand current cyber issues from a senior executive's perspective
- Be able to collaborate with interdisciplinary teams toward project completion
- Identify a topic and required resources to complete a multi-disciplinary M&S capstone project in the Fall

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

IDC 6600 focuses on emerging topics in cybersecurity by examining current events through the use of guest speakers that are subject matter experts in the field. This course further builds upon the first three courses in the certificate by focusing more heavily on the current issues facing cybersecurity specialists today and how modeling and simulation techniques can possibly address those challenges. More info on the graduate certificate program can be found at - <http://www.graduatedatalog.ucf.edu/programs/program.aspx?id=11981>. 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.

III. Course Requirements

- **Syllabus Quiz (5 points)**

Take the online syllabus quiz during the first week of class. You can take the quiz more than once; the highest grade obtained counts.

- **Reaction Papers (70 points - 7 x 10 points)**

Students will work independently for the entirety of the course. After the guest lecturer's class is conducted, each student will write a paper individually (due on the following Sunday) and post their reaction. Did the speaker answer the question fully? How did the speaker do overall? Impressions? Pros/Cons of the speaker's talk? And, would you recommend asking them back for next year's class?

Please use the following template to complete your reaction paper assignments. Also, ensure your papers are at least one page in length, single-spaced:

[Template for Reaction Papers.docx](#)

- **Emerging Cyber Issues Research Topic Proposal (25 points)**

Write a proposal for an emerging cyber issues research study you would like to perform in the near future (you will not actually conduct the study in this course). You will write a proposal that describes the rising cyber issue, what you would like to investigate (research question), define the purpose and motivation of the study, describe the current state of the issue/threat and countermeasures, and define your experiment methodology.

IV. Evaluation Method and Grading

We use a +/- scale based on a percentage of total points. See the graph below. Assignments will be graded on a point system - 100 points max.

Late assignments are not accepted. There will be one make-up assignment at the end of the semester.

We will do our best to give prompt feedback to your work so that you are able to know how you are doing as the course goes on. Take advantage of the rubrics for assignments, as they will guide you to achieving maximum credit for your work.

Grade postings: All grades will be posted on Webcourses.

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

V. Reading Material

No mandatory textbook.

However, the material that will be used for this class will mainly consist of academic and military texts and information sources:

- Cybersecurity National Action Plan, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
- National Cyber Strategy, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- DoD Cyber Strategy Summary, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
- Federal Bureau of Investigation's Cyber Crime Info Page, <https://www.fbi.gov/about-us/investigate/cyber>

VI. Other Useful Resources

- School of Modeling, Simulation and Training, <http://www.ist.ucf.edu>

- United States Computer Emergency Readiness Team (US-CERT), <https://www.us-cert.gov>
 - United States Army Cyber Center of Excellence, Fort Gordon, Georgia, <http://cybercoe.army.mil>
-

VII. Miscellany

- **Academic Honesty**

I expect a high level of integrity and honesty in this course. See UCF Golden Rules for specifics at <http://goldenrule.sdes.ucf.edu>

- **Copyright**

This course may contain copyright protected materials such as audio or video clips, images, text materials, etc. These items are being used with regard to the Fair Use doctrine in order to enhance the learning environment. Please do not copy, duplicate, download or distribute these items. The use of these materials is strictly reserved for this online classroom environment and your use only. All copyright materials are credited to the copyright holder.

- **Disability Statement**

The University of Central Florida is committed to providing reasonable accommodations for all persons with disabilities. This syllabus is available in alternate formats upon request. Students with disabilities who need accommodations in this course must contact the professor at the beginning of the semester to discuss needed accommodations. No accommodations will be provided until the student has met with the professor to request accommodations. Students who need accommodations must be registered with Student Disability Services, Student Resource Center Room 132, phone (407) 823-2371 **Error! Filename not specified.** (407) 823-2371, TTY/TDD only phone (407) 823-2116 **Error! Filename not specified.** (407) 823-2116, before requesting accommodations from the professor.

- **Third-Party Software and FERPA**

During this course, you might have the opportunity to use public online services and/or software applications, sometimes called third-party software, such as a blog or wiki. While some of these could be required assignments, you need **not** list any personally identifying information on a public site. Do not post or provide any private information about yourself or your classmates. Where appropriate, you may use a pseudonym or nickname. Some written assignments posted publicly may require personal reflection/comments, but the assignments will not require you to disclose any personally identifiable information. If you have any concerns about this, please contact the course instructor.

- **Modifications**

The instructors reserve the right to modify the syllabus at any time.

