I. Course Information

- Course Number - Title: ***IDC 6601 - Behavioral Aspects of Cybersecurity***
- Credit Hours: 3.0
- Semester/Year: Summer 2021, Session "C" (2 sections - "M" and "W")
- Location: Lectures will be held online for both "M" and "W" sections each Wed in the Summer "C" term from 5pm to 7:50pm. Lectures are recorded each week in Zoom.

- **Intructor:** Bruce Caulkins, Ph.D.
- **Office Hours:** By appointment
- **Email:** Use Webcourses

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
- Apply appropriate analysis techniques to data to spot insider threats
- Understand cyber hacker motivations and techniques
- Be able to collaborate with interdisciplinary teams toward project completion
- Write research reports/articles

Description: This is a core course for the Graduate Certificate in Modeling and Simulation of Behavioral Cybersecurity. IDC 6601 focuses on human, social, and behavioral issues related to cybersecurity including organizational management techniques, motives for cyber crimes, risk and threat analysis, and ethics and legal issues. Top modeling and simulation techniques and some relevant psychological issues including human systems integration and human computer interaction will be applied as they relate to securing data, computers, and the networks on which these reside.

This course further builds upon the first two courses in the certificate by focusing more heavily on the human aspects of cybersecurity and how modeling can address those challenges. More info on the graduate certificate can be found at - 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.

III. Course Requirements

- **Syllabus Quiz (5 points)**
- **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. Focus less on your bio information since you have given this information out before and focus more on the class and what you expect to get out of it and why.

- **Assignments (43 points total) - 3 each worth 10, 15, 18 points**

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

- **Presentation (10 points) - 1 each**

Each student will give a ten-minute (max) oral presentation (with slides) to the class on their answer/take on one of the three assignments. Online students must also create a briefing but with substantial comments in the Notes section of each non-tile slide in the PowerPoint slideshow. **I will ask for volunteers but check your Webcourses' inbox frequently as I may assign folks to give a presentation in case I do not get enough volunteers.** There are three assignments and I would like an equal number of presentations (approx) for each assignment.

- **Discussions (20 points) - 4 each worth 5 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. It will be turned in as a written report.

IV. Evaluation Method and Grading

We use a +/- scale, based on percentage of total points. See graph below. Assignments, presentation, discussions, and final exam will be graded on a point system - 100 points max. No extra credit is given and 1 point off work for every day late.

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.

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:

- National Cyber Strategy, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Links to an external site.)
- DoD Cyber Strategy Summary, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Links to an external site.)
- Federal Bureau of Investigation's Cyber Crime Info Page, https://www.fbi.gov/about-us/investigate/cyber
- Joint Publication 3-12 (R), "Cyberspace Operations," http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

---

VI. Other Useful Resources

- DARPA Cyber Grand Challenge, https://cgc.darpa.mil
- Department of Homeland Security, Cybersecurity, http://www.dhs.gov/topic/cybersecurity
- Institute for Simulation and Training, http://www.ist.ucf.eduLinks to an external site.
- SANS Reading Room, http://www.sans.org/reading-room/
- 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**

We expect a high level of integrity and honesty in this course. See UCF Golden Rules for specifics at http://goldenrule.sdes.ucf.eduLinks to an external site.

- **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 (407) 823-2371, TTY/TDD only phone (407) 823-2116 (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 one of the course instructors.