HACS 208Y: Cyber Psychology

Thursdays, 9:30AM – 12:15PM
Prince Frederick Hall 1111

Dr. Dana S. LaFon
Senior Behavioral Scientist
dslafon@ic.fbi.gov
Phone: 410-277-6764

Course Materials:
- Executive Order 13707: Using Behavioral Science Insights to Better Serve the American People (available online)
- Social Media articles provided in class
- Research in class

Course Description:
Behind every cyber event is a human or group of humans with their own motivations, goals, and ideologies. This course focuses on understanding how behavioral science can be leveraged to understand, anticipate, and defend against the adversary in a national security setting. The science of influence, social media, behavioral analysis/profiling, and ethical considerations will be covered. The class is based on lectures and discussions. Outside of the classroom, the expected method of communication is the use of Canvas.

Course Goals:
The main goal of the course is to understand how behavioral science can be leveraged to understand, anticipate, and defend against the adversary in a national security setting. The science of influence, social media, behavioral analysis/profiling, and ethical considerations will be covered.

Grading and Assignments:

Grading

Participation (10%)
Kobayashi Maru Exercise (10%)
TRASHINT/Presentation (20%)
Spearphishing Exercise/Presentation (20%)
CNE Exercise/Presentation (20%)
Integration Paper (20%)

Please see the undergraduate catalogue for a description of grades, e.g. A+, A, A-, etc.: http://www.umd.edu/catalog/index.cfm/show/content.section/c/27/ss/1584/s/1534

Assignments

Participation in Class Discussions:
This course requires that you actively participate. This is accomplished by attending class, listening to discussions, contributing your thoughts to the discussion, commenting on others’ expressed points of view, actively contributing (and sometimes leading) group activities and presenting to the class according to assignment instructions.

Kobayashi Maru Exercise:

Understanding the mindset of others is a major construct in psychology. Without the ability to understand not just how others think, but also how they are influenced by their environment, their surroundings, and group pressures, it is impossible to empathize their paradigm. One significant difference between many cyber actors, be they state actors or hacktivists, is the difference in rule sets. The United States has significant policies and procedures in place to protect, but which often limits certain activities. Additionally, and this is a generalization on my part, those who seek government type jobs, analyst positions, and even students (shocking, I know) tend to be rather rule based from the start. Thus, asking an employee rule-follower to follow more rules may restrict one’s thinking. When we attempt to understand our adversaries, we often start by applying our own cognitive biases and belief systems of what is right/wrong or allowed/unallowed. This can be dangerous as oftentimes our adversaries do not play by the same rule book we must follow, or, in some cases, as in cyber crime, there are no rule books at all.

The Kobayashi Maru exercise is drawn from a fictional depiction of an impossible test in which there was no winning solution. The goal of the fictional exercise was to see how a leader would react in a no win situation. However, our hero chose to win by cheating the no win scenario. We don’t often get a chance, nor are we encouraged, to cheat. Thus, we don’t think outside the rules box very often. You will be asked to think outside your traditional rule based paradigm for this exercise. You will be given a no win scenario and are asked to find a cheat solution. You will be quizzed on the computation of pi to the 100th decimal in a closed book, cleared desk quiz. You will turn in your solution on a single blank page. Then you will each share your cheat method with the class. You are judged on creativity of the cheat. The more creative the cheat, the more points you earn. Points will be given by the class and the professor. Each student has one vote and will not be allowed to vote for him or herself. The professor gets two votes... just because I can. The winner will be amply rewarded with the coveted Kobayashi Maru t-shirt, as well as passing the exercise with 10 extra credit points. The grading rubric for this exercise is quite simple. Put some creativity into your cheat and you pass. Don’t cheat means you don’t pass the assignment. (Assignment is pass/fail.)
TRASHINT Exercise

What can we learn from trash?
The “INT” of the Intelligence Community is shorthand for intelligence. Intelligence gathering is part of the role of the intelligence community. NSA does SIGINT (i.e. Signals Intelligence), CIA does HUMINT (Human Intelligence), and so on. These “INTs” are based on the concept that intelligence can be gathered by a variety of methods. Collecting multiple pieces of information can add up to a sum greater than the whole. This is the gestalt of intelligence gathering. This is a group exercise. As a group, you will decide how to acquire your targeted intelligence which will be announced in class. Once your trash intelligence is acquired, you will bring it to class to examine and derive what intelligence insights you can learn from its contents. You will assess the intelligence for information related to your mission, which is to develop an influence strategy targeting the group from which the intelligence was acquired. The influence strategy is to be based on the influence psychology principles learned in class. Mission and target will be expanded upon in class. Influence strategies will be presented in week 12.

Spear-phishing Exercise

Who falls for Spear-phishing? You tell me. This exercise involves investigation on both technical and social science research on what makes an effective spear-phishing campaign. This will be researched in class as a group (in pairs) and will require some individual research outside of class. The groups will decide how to organize the research. Based on what you learn through your research and in-class discussion, each group will devise an effective spear-phishing campaign against another group (not the professor!). In one class session we will research and discuss. Outside of class, your group will devise and launch your spear-phishing attack. Two class sessions later, each group will present their spear-phishing methodology to include the primary social engineering principles, psychology constructs, and case studies on which they based their methodology. Each group will be graded on the thoroughness of their literature review, the application of their research, and extra credit of 5 points will be rewarded for each group member whose spear-phishing attempt was successful.

Who’s behind the CNE?
Find the human behind the CNE – group exercise (in pairs). Select a cyber-attack that has occurred and trace its origin to the “who” (i.e. group and/or individual) and how influence psychology and motivation was used. In pairs, you will select and examine an example of a Computer Network Attack. You will present to the class the incident (what and how it happened), the individual, group and ideology/motivation behind the attack (the who), the victim (who, where) and the timeline of the attack (when). You will be expected apply the research from class onto the method of the CNE and judge how well the attackers applied these principles and how successful they were. You will be graded on your depiction of the incident and all its components, how well you applied the principles you’ve learned in class and your assessment of how well the attackers did and what they could have done to improve their methodology.

Integration Paper
You are to write a 3-4 page paper (not including references) applying the Cialdini influence principles to the Hadnagy Phishing Dark Waters text and the spear-phishing influence strategy you devised. Papers are to be written individually. Compare and contrast how Cialdini’s principles are reflected and/or refuted in Hadnagy constructs he presents in his text and how you incorporated them into your influence strategy. Papers are due to the Professor on Week 14 (28 April). You may email them or turn in a hard copy by Week 14.

Course Schedule

Week 1 (28 Jan)

Introduction to Course/Professor/Students

Readings Due:
Executive Order 13707: Using Behavioral Science Insights to Better Serve the American People (Each student is to bring a print out of this to class)

A review of Social Media Psychological Research: What does your online presence say about you?
One of the primary contributions of the field of psychology is its scientific rigor in understanding the human-how we think, act, and feel. How we present ourselves can tell us a great deal about one another, but the perceptions we gather from what others present or “leak” about their own personality characteristics must be understood from a rigorous scientific perspective. Hunches, assumptions, and “gut feelings” have no place in psychology. They are wrought with bias.
The field of psychology has produced a great deal of research examining how to understand each other from what we present online and, specifically, in social media. You will be presented a review of this research and provided a guided understanding of how to be an educated consumer of this research.

Kobayashi Maru Exercise Assigned
TRASHINT Exercise Assigned: What do you need to know to accomplish your mission?

Week 2 (4 Feb)

Understanding Another Mindset: Mindset of the Adversary
Criminal Profiling in Cyber
  FBI Behavioral Profiling
  Pattern of Life
  Debunk CSI Effects

Kobayashi Maru Exercise
Postponed (TBD): Behavioral Artifacts in metadata: How do you exploit metadata for behavioral components?
SSA Cameron Malin, CBAC Lead, FBI, author:
*Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides*
Malware Exercise LavaTiger

**Week 3 (11 Feb)**
TBA

**Week 4 (18 Feb)**
*Cyber Denial and Deception Guest Speakers Dr. Kristen Heckman and Dr. Frank Stech, MITRE Corporation*

The use of Denial and Deception practices have been part of warfare for centuries. But how is this age old tactic useful in cyber? Drs. Heckman and Stech, are on the cutting edge of this field. They will be providing insight into how this work is calibrated in cyber and leveraged to support national security.

**Week 5 (25 Feb)**
*TRASHINT Exercise: TRASHINT Part One: Discovery*

**Week 6 (3 Mar)**
*Insider Threat: Mindset of a Spy*

(Field Trip across campus) *Using online and kinetic behavioral correlates to identify insider threat in CBRN scenario: ODNI IC Post-Doctoral Fellowship Program lead by FBI/NSA.*
Meet/discussion with PI Dr. Cory Davenport, UM START Consortium

Readings Due:
PERSEREC Study, 2008

**Week 7 (10 Mar)**

Required Reading Due:

Preparation for Psychology of Influence: In preparation for our section on the psychology of influence, each student will research the psychology body of literature (peer reviewed journals only) for a research article on influence. Each student will locate, read, and discuss their article
with the class in week 10. Since this is a small class, coordinate amongst yourselves so there are no duplications. (Counts as part of students’ class participation grade).

Prepare TRASHINT Presentations

Week 8 (17 Mar)

Spring Break 😊

Week 9 (24 Mar)

State of the art in Industry for threat assessment electronically

Guest speaker from Industry

Threats are no longer just on the news in another place. Now they can reach you in your home or at work. They can be a coworker, or someone you met on Facebook. How can you distinguish this type of behavior online when there is a faceless person on the other end? How can you tell a threat from a hoax? Why would someone become involved in cyber espionage?

Week 10 (31 Mar)

Introduction to Psychology of Influence

Class Discussion of Readings

Understanding the psychology of influence and persuasion is essential to social engineering constructs. We will review and discuss the strategies learned from the field of psychology as well as share our influence articles with the class.

Student Influence Article Presentations

Week 11 (7 Apr)

Required Reading Due

Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails

Social Engineering and Influence

In class case study: Anonymous: How do they use Social Engineering?

Spearphishing Exercise

Week 12 (14 Apr)
**TRASHINT Part II: Influence Strategy Presentations**

**Research in the Field of Psychology and Intelligence**

Guest Speaker:
Intelligence Advanced Research Program Activities (IARPA) Program CAUSE: Exploiting sensor data to anticipate digital threats automatically (Robert Rahmer, CAUSE Program Director)

**Week 13 (21 Apr)**

*Spear-phishing Exercise Part Two: Presentations*

**Whose behind the CNE? Part One: In class research**

**Week 14 (28 Apr)**

*CNE Exercise Presentations*

Integration Papers Due

**How do government pay scales work?**

Getting a job/clearance/career

**Wrap up and final open academic and career discussions**

**Week 15 (12 May)**

Finals Week: No Class

**Final Exam**

There is no final exam for this course.

**Course Procedures and Policies**

*Attendance and absences:* Students are expected to inform the instructor in advance of medically necessary absences, and present a self-signed note documenting the date of the missed class(es) and testifying to the need for the absence. This note must include an acknowledgement that (a) the information provided is true and correct, and (b) that the student understands that providing false information to University officials is a violation of Part 9(h) of the Code of Student Conduct.

Prolonged absence or illness preventing attendance from class requires written documentation from the Health Center and/or health care provider verifying dates of treatment when student was unable to meet academic responsibilities.
Absence due to religious observance will not be penalized, however, it is the student’s responsibility to notify the instructor within the first 3 weeks of class regarding any religious observance absence(s) for the entire semester.

**Academic integrity:** The student-administered Honor Code and Honor Pledge prohibit students from cheating on exams, plagiarizing papers, submitting the same paper for credit in two courses without authorization, buying papers, submitting fraudulent documents and forging signatures. On every examination, paper or other academic exercise not specifically exempted by the instructor, students must write by hand and sign the following pledge:

> I pledge on my honor that I have not given or received any unauthorized assistance on this examination or assignment.

Allegations of academic dishonesty will be reported directly to the Student Honor Council: [http://www.shc.umd.edu](http://www.shc.umd.edu)

**Students with disabilities:** The University of Maryland is committed to providing appropriate accommodations for students with disabilities. Students with a documented disability should inform the instructors within the add-drop period if academic accommodations are needed. To obtain an Accommodation Letter prepared by Disability Support Service (DSS), a division of the University Counseling Center, please call 301-314-7682, e-mail dissup@umd.edu, or visit the Shoemaker Building for more information.

**Copyright notice:** Class lectures and other materials are copyrighted and they may not be reproduced for anything other than personal use without written permission from the instructor.

**Emergency protocol:** In case of an emergency where the University is closed, assignments that were assigned before the closure will still be due electronically. If the University is closed, class will not meet but students are responsible for checking Canvas and/or their e-mail regularly for further instruction regarding make up assignments and schedule changes. The professor will communicate updates to the syllabus if necessary.

**This syllabus is subject to change.** Students will be notified in advance of important changes that could affect grading, assignments, etc.

**Course evaluations** are a part of the process by which the University of Maryland seeks to improve teaching and learning. Your participation in this official system is critical to the success of the process, and all information submitted to CourseEvalUM is confidential. (Instructors can only view group summaries of evaluations and cannot identify which submissions belong to which students.)

**Academic Accommodations for Students Who May Experience Sexual Misconduct:**
The University of Maryland is committed to providing support and resources, including academic accommodations, for students who experience sexual or relationship violence (as defined by the University’s Sexual Misconduct Policy). To report an incident and/or obtain an academic accommodation, contact the Office of Civil Rights and Sexual Misconduct at 301-405-1142. If you wish to speak confidentially, contact Campus Advocates Respond and Educate (CARE) to Stop Violence at 301-741-3555. Disclosures made to faculty are not confidential and must be reported to the Office of Civil Rights and Sexual Misconduct. For more information visit www.umd.edu/Sexual_Misconduct/.

Diversity: The University of Maryland values the diversity of its student body. Along with the University, I am committed to providing a classroom atmosphere that encourages the equitable participation of all students regardless of age, disability, ethnicity, gender, national origin, race, religion, or sexual orientation. Potential devaluation of students in the classroom that can occur by reference to demeaning stereotypes of any group and/or overlooking the contributions of a particular group to the topic under discussion is inappropriate.