Cyber Threats and Intelligence
CEHC 469/569 – RPAD 569
Spring 2019, HS202 M5:45-9:25

Professor: Stacey A. Wright, CISSP
swright@albany.edu

Course Summary and Objectives
Over the past two decades cybersecurity has transitioned from being the purview of computer nerds and information technology (IT) departments to requiring special knowledge, skills, and abilities. Similarly, cybercrime has undergone a series of radical shifts from any crime involving computers to the current definition which often focuses on computer network intrusions. Cybercrime currently involves a range tactics, techniques, and procedures (TTP) from the introduction of malware into networks through varying delivery mechanisms, to distributed denial of service (DDoS) and Structured Query Language (SQL) injection (SQLi) attacks. Motivations run the gamut from financial gain to notoriety, social activism, espionage, and revenge.

Preventing, mitigating, and responding to cyber incidents requires a thorough understanding of the risk equation, encompassing both the threats and the vulnerabilities. Company executives, managers, and communication liaisons, as well as the human resources, IT, finance, security, and legal departments, many of whom have limited experience with or understanding of incidents, are often involved in the response. By understanding the myriad cyber threats and motivations, leaders can guide organizations in accurately determining risks, minimize the potential for incidents, and, when necessary, provide more thoughtful responses to incidents.

This course will examine cybersecurity risk from the threat side of the risk equation. Students will be introduced to the different types of threats, with a special focus on today’s actors, motivations, and TTPs, while gaining insight into the impact of cybercrime on victim organizations and employees. A variety of case studies will be used to study threats to organizations, why TTPs are chosen, and attack consequences. As a course in the Intelligence field, students will receive an introduction into intelligence analysis and receive a variety of tools to aid them in understanding the foundation of cyber threat intelligence (CTI).

Students attending this course should be familiar with the structure of the Internet and willing to learn technical information. This is not a technical course but the course will require students to understand technical information at a high-level.

Pre-requisites:
There are no pre-requisites. Undergraduate students must be at least Juniors and have the instructors permission.

Office Hours
I do not have an office on campus. Therefore office hours are before and after class, in the classroom, as needed. If you need additional time or a different day, we will arrange something mutually convenient for us both, on campus or via telephone.

Each student will have the opportunity to work one-on-one with me to outline their final paper and receive assistance.
Grading:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Component</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td>Class Attendance and Participation</td>
<td>Attendance is expected. If you know you're going to be absent, notify the professor. Participation is expected and includes both participation in lecture and in group activities and exercises. University Medical Excuse Policy</td>
</tr>
<tr>
<td>25%</td>
<td>Homework Assignments</td>
<td>A variety of homework assignments will be given throughout the semester. Completing these is vital to understanding and participating in the class.</td>
</tr>
<tr>
<td>25%</td>
<td>Case Studies</td>
<td>Two assigned case studies.</td>
</tr>
<tr>
<td>25%</td>
<td>Case Analysis Term Paper and Presentation</td>
<td>- A list of topics to select from will be provided</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Topic due 4th class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Intel Question Form due 5th class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Outline due 8th class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Paper due last class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Presentation during final exam period</td>
</tr>
</tbody>
</table>

Class Content, Readings, and Homework Assignments:
All readings and assignments are subject to change due to ongoing events and will be posted on Blackboard. Reading material will be available through the Internet and does not require purchase of a book. In some cases, the readings may be made available on Blackboard for your convenience or the readings may consist of watching instructional videos.

All assignments are to be submitted via email to the Professor, before class starts, unless otherwise noted. Assignments should include, at a minimum, the student's name, date the assignment was given, class number, and complete answers to the all questions posed. Arial 11pt font, single-spaced text is preferred. Assignment grades are based on the student's thoroughness in answering the assigned questions and inclusion of class and reading content. Proper citations are required. Failure to properly cite references will result in a penalty.

Additional Readings
A list of additional sources for more information will be posted in Blackboard.

Students with Disabilities
Reasonable accommodations will be provided for students with documented physical, sensory, systemic, medical, cognitive, learning and mental health (psychiatric) disabilities. If you believe you have a disability requiring accommodation in this class, please notify the Disability Resource Center (518-442-5490; drct@albany.edu). Upon verification and after the registration process is complete, the DRC will provide you with a letter that informs the course instructor that you are a student with a disability registered with the DRC and list the recommended reasonable accommodations.

Academic Integrity:
It is every student's responsibility to become familiar with the Standards of Academic Integrity at the University. Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity.

Plagiarism: Presenting as one's own work the work of another person (for example, the words, ideas, information, data, evidence, organizing principles, or style of presentation of someone else). Plagiarism includes paraphrasing or summarizing without acknowledgment, submission of
another student's work as one's own, the purchase of prepared research or completed papers or projects, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

**Class Schedule:**

1st Class - Class introduction
- Class introduction
- Intelligence, intelligence analysis, CTI
- Words of Estimative Probability

2nd Class – Cyber TTPs and Terminology
- What are the common TTPs and vectors? How do they work?
- Cyber standards, practices, and models

3rd Class – Biases, Mindsets, and Assumptions
- What are our biases, mindsets, and assumptions? How do they affect our responses?
- What tools can we use to prevent, be aware of, or offset them?
- Scope Notes
- Key Assumptions Check

4th Class – Cybercriminals and Monetizing Cybercrime
- Topic choice due
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
- How do you monetize cybercrime?
- Analysis of Competing Hypothesis (ACH)

5th Class – Hacktivism and Sourcing
- Intel Question Form due
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
- When is hacktivism wrong? When is it right?
- Quality of Information Check
- Sourcing and Source Summary Statements

6th Class – Insiders
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
- Brainstorming
- Quadrant analysis

7th Class – Terrorists
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
- High-impact/low-probability analysis (black swan events)
- Alternative Analysis

8th Class – Nation-State Actors: Russia and China
- Outline due
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
Signposts of Change

9th Class – Nation-State Actors: Iran and North Korea
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?
- Red teaming/Mirror imaging

10th Class – Criminals
- What is the threat? What motivates them? Why? Who is at risk? What TTPs do they use?

11th Class – Intelligence Challenges and Failures
- What makes intelligence analysis and CTI so difficult?
- When does it go wrong?
- What can you do about it?

12th Class – Putting It All Together

13th Class – Countering Cybercrime
- Paper due
- Roles, responsibilities, and ethics

Final Exam period – Individual Case Study Presentations

Stacey A. Wright
January 2019