Course Summary:

Our world is more connected today than it has ever been in our history. Tomorrow we will be more connected than we are at this very moment. While each connection we make in the virtual world is intended to make our lives easier, we must ask ourselves, “What if someone pulled the plug? How do we respond? Should we have been able to prevent it?”

Since the creation of electronic devices that transmit information there have been criminals, terrorists, and nation states that seek to exploit them for financial, social, or political/ideological gain. This threat has become one of the top national security priorities, requiring a cyber force that includes the training of people who don’t even work as cyber professionals. Maybe you have seen the signs in your current work places, “Security is everyone’s responsibility.” A simple statement has never been truer.

This class is intended to paint a broad brush of the cyber security landscape and introduce you to the many aspects of how cyber security is viewed by industry, private sector business, civil government, military, and academia. The class will also provide a cursory overview of technical knowledge of the underlying systems used to implement cyber security.

Students taking this class will be well equipped to take more advanced technical courses in a multitude of disciplines that make up cyber security. It will also provide the more technically advanced students an opportunity to better understand the management, policy, and political equities involved in cyber security from a mid-micro to macro organizational level.

Most of the interaction between cyber security experts and the clients they serve is conducted via video teleconference. So it is fitting that this course is being offered online. As a class we will work to operate in a professional format that in most cases mimics real world situations. This will be the best way to bring the real world into our virtual classroom.

Below you will find a weekly break down of assignments and topics to be covered as well as what are required of you each week. Each week is annotated with a “pre-record” or “live” tag. If it is a pre-record please feel free to watch or listen to lectures at your leisure. If it is a live discussion it is highly encouraged that you log in and participate. If a live discussion is canceled, it will be replaced with a pre-recorded lecture on the same topic, or a pre-recorded lecture from a new topic will take its place. If a live discussion is canceled and there is an assignment due that day, you must still complete the assignment.
There will be a total of four live sessions all held on Wednesdays which are highlighted in bold on the class schedule.

**Class Delivery Platform:**

Our class will use a combination of Adobe Connect and Blackboard. Blackboard will be used as the primary means of content delivery. Assignments, lectures, materials, and forum discussions will all be held using Blackboard.

Adobe Connect will be our platform for live interactive communication. You will receive login instructions prior to the first class meeting which will be held in a live Adobe Connect session.

**Assignments:**

**Weekly Cyber/Cyber Security News Article** – Every week, each student will seek out a specific news article related to cyber security to post. With the post, each student should write a half to full-page analysis of why this article is important. What are the impacts to a particular industry, demographic, region, etc? This is not a summary, use your analytical skills. During live sessions 1-3 students will be asked to present their article to the class. Articles should be posted by Wednesday of each week.

**Weekly Discussion** – Every week students will be required to post 3 comments on a class discussion thread. Comments should be no less than one paragraph in length. The topic will relate to that week’s subject area. Students are encouraged to engage each other in discussions that further analytical and creative ideas. Discussion opens on Sunday night and close on Friday at midnight. This leaves Saturday as an open day.

**Memo Assignment #1** – Students will be provided a scenario which they must research and provide a synopsis to senior level leadership on multiple cyber threats impacting a particular interest.

**White Paper** – Students will be required to pick a cyber security related topic, take a position, and argue it to a specified audience through the use of a white paper. A list of potential topic areas will be provided but it is encouraged that each student find a unique and timely topic. Topics will be submitted for consideration and approval in week six.

**Group VTC Role Play** – All students will participate in a real time VTC scenario that will be provided in advance so that key players can prepare. Scenarios will include Chief Information Officers (CIOs), CEOs, Directors, Managers, Intelligence Analysts, Senior Military Leadership, etc.

**Memo Assignment #2** – Students will be provided a scenario which they must research and provide a decision(s) to respond to a threat imposed on a particular interest.
**Memo Assignment #3** – Students will be provided a scenario which they must research and provide an after action report to senior leadership.

**Capstone Project** – The entire class will meet in person at the Rockefeller College downtown campus to complete an interactive simulation as part of the capstone project. The class will be broken up into an Executive Board of senior officials of a government agency, and two groups that are to provide cyber security solutions for a specific scenario concerning the organization. This will be an expedited real-time scenario run over the course of two days. There will be specific milestones that must be reached. Some milestones will be set beforehand but all other milestones will be driven by the class as it conducts the simulation. The capstone will be proctored by the instructor and other Rockefeller College faculty members. A deeper review of the group and individual grading process will be covered prior to the capstone project.

**Grades:**

- Participation: 20%
- Written Assignments: 25%
- Online Discussion: 15%
- Capstone: 40%

_Students enrolled in the undergraduate section of this course (RPAD 445 rather than RPAD 545) will be expected to participate in all in-class and homework individual and team exercises. Reading requirements, however, will be significantly less demanding for the undergraduate section. Finally, undergrads will be judged by different criteria for grading._

**Weekly Breakdown:**

**Week 1**

Course overview and administration. Provide an overview of all the assignments and the schedule of completion for those assignments. Discuss cyber security. What is cyber security? (Pre-Record)

**Week 2**

Access Control and Identity Management – The lecture will focus on Access Control methodologies and implementation across all types of networks. Identity Management will focus on methodologies of security used in information systems (IS). (Pre-record)

**Week 3**

Cyber Security: The Issues – Discussion will focus on the implementation of security. Questions we will explore are as follows. Are we leading or falling behind? Can the government regulate
cyber security measures for critical infrastructure and key resources (CI/KR)? Should the private sector be forced to hand over data to government agencies? Should the private sector be allowed to conduct cyber espionage or cyber warfare to protect their interests? If not how do you prosecute them? (Live)

**Week 4**

Cryptography – This lecture will focus on basic telecommunications systems and network security methodologies. The history of cryptography will also be covered. (Pre-record) (Memo #1 Due)

**Week 5**

Cyber Security in Government – Who does what? Discussion will focus on the function of cyber security within government (Federal, State, and Local). Also what are the responsibilities of specific agencies at the federal and state level? (Live)

**Week 6**

Threats and Vulnerabilities – This lecture will focus on Threats and Vulnerabilities related to cyber security. (Pre-record)

**Week 7**

Application, Data, and Host Security – The lecture will cover Application, Data, and Host Security methodologies and implementation strategies. (Pre-record) (Whitepaper due)

**Week 8**

Compliance and Operational Security – The lecture will cover business continuity methodologies and disaster recovery plans for all private industry and government. The lecture will cover the various laws that are in place which must be followed by government and/or private industry. Governance and risk management are key aspects of compliance with laws and regulations put in place to protect information systems. (Pre-record) (Memo #2 Due)

**Week 9**

BREAK

**Week 10**
Cyber Warfare and Intelligence – Discussion will focus on how cyber intelligence integrates with other traditional forms of intelligence. What types of cyber intelligence exist? The class will explore how federal agencies, military, and state agencies contribute to cyber intelligence. Group VTC roles assigned. Discussion will focus on the hottest topic in cyber security today, the new domain of warfare. This discussion will spark much debate and be a great lead in to the Group VTC scenario and Capstone Project. (Pre-record)

**Week 11**

Cyber Warfare and Intelligence – Discussion will focus on how cyber intelligence integrates with other traditional forms of intelligence. What types of cyber intelligence exist? The class will explore how federal agencies, military, and state agencies contribute to cyber intelligence. Group VTC roles assigned. Discussion will focus on the hottest topic in cyber security today, the new domain of warfare. This discussion will spark much debate and be a great lead in to the Group VTC scenario and Capstone Project. (Live) (Memo #3 Due)

**Week 12**

Cyber Policy Development – This lecture will focus on key components of the cyber policy development process. This will be vital to the capstone project.

**Week 13**

Overview of Capstone Project (pre-record) (white paper due).

**Week 14**

Catch up week

**Week 15**

Capstone Project held at Rockefeller Campus