**INTA 4803/8803SG,
Networks, Infrastructures, and Security**

Spring 2018
Weds, 3:00 – 5;45 pm, 136 Habersham

Prof. Seymour E. Goodman,
seymour.goodman@inta.gatech.edu, 302 Habersham, 5-1461

Prof. Dennis Lockhart, dennislockhart@earthlink.net

Jonathan Darsey, jonathan.darsey@gatech.edu, 116-B Habersham.

This syllabus is current as of January 3, 2018

**Course Description**:

A more networked world has emerged since the end of the Cold War. Political, military, social and economic conflict, cooperation, and well-being are increasingly affected by the pervasive presence and availability of dense and large-scale networks.

We will generalize “security” beyond that of protection from malicious actors to include other forms of protection and assurance: safety, survivability, sustainability, resilience, reliability, response, renewal, robustness, and recovery.

We define infrastructures as large scale networks for creating and delivering goods and services, and 10-20 of these have been deemed so important that they have been declared Critical Infrastructures (CI). Among these are civil aviation, banking and finance, electric power, oil and gas, water and sewage, highways, bridges etc., and communications infrastructures ranging from telephony to the public media to the Internet of Things. For vast numbers of people and organizations around the world, CIs operationally define modern civilization and globalization.

Most of the physical infrastructures have information infrastructures deeply embedded in them. Some have gotten to the stage where the physical infrastructures may be increasingly seen as being built around the information infrastructures. As such the vulnerabilities and insecurities that plague information infrastructures are inherited by the physical infrastructures. The course will thus necessarily include an overview of the landscape of cyber security.

The class as a whole will consider three case studies in detail: (1) The CI dimensions of the 9/11 attacks, arguably the most important national and international security event since World War II; (2) civil aviation; and (3) electric power grids. Other CI will be studied as substantial student projects.

We expect to have about a half dozen guest presentations from people with real world responsibilities for the well being of critical infrastructures.

**Learning objectives**:

This course has three major learning objectives.. The first objective is to build content knowledge, developing a picture of both the ‘trees and the forest’ for specific areas of critical infrastructure. This content knowledge includes:

* Defining and categorizing the different types of critical infrastructures embedded in modern society
* Identifying weaknesses in different infrastructures, including those vulnerabilities and access points that malicious actors could exploit
* Describing connection points and dependencies linking different critical infrastructures
* Assessing the degree to which certain groups of critical infrastructures operate as networks, with the attendant strengths, weaknesses and uncertainties inherent in complex dynamic systems.

The second learning objective is to develop skills required to engage with ‘wicked problems’ such as CI--problems that have enormous importance, scope, complexity and uncertainty. We will build these skills by utilizing tools and approaches such as:

* For risk assessment:
	+ Network maps & models
	+ Risk / vulnerability assessments
	+ Impact estimations (direct & indirect disruption costs)
* For risk mitigation:
	+ Scenario planning, including for ‘Black Swans’ (low probability, high impact events)
	+ Contingency / continuity planning.

The third learning objective is to enhance many of the top abilities that employers expect from the students they hire. These include, in order, the abilities to:

* work in teams
* verbally communicate inside and outside of the organization,
* solve problems and make decisions,
* obtain and process information,
* plan, organize and prioritize work,
* analyze quantitative data, technical knowledge related to the job,
* proficiently use software,
* create and/or edit reports,
* influence others.

Our class will give emphasis to developing a mix of these abilities in a challenging and less certain context than you are used to. Working under that uncertainty is an important part of stretching you in all of the ways listed above.

**Common Sources**:

***The 9/11 Report, The National Commission on Terrorist Attacks Upon the United States,*** New York Times edition, St. Martin's Paperbacks, 2004. (Any edition will do.)

Ted Koppel, ***Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath***, Crown, NY, 2015.

Video: “Eye in the Sky” (full length feature movie)

Each student should identify a small number of media sources (broadcast, printed, social, other?) that regularly cover massively disruptive events and follow those throughout the semester. Starting with the third week, the final 15-20 minutes of every Thursday class will be devoted to discussing relevant events and developments that have arisen in the preceding week or two.

Each team is expected to find and record, as an annotated bibliography, source material on their specific subject.

**Grading**:

Grading will be based on a combination of individual and group assignments. The breakdown is as follows:

25% Class participation, including attendance.

20% Short individual writing and presentation assignments to be given over the course of the semester.

50% Team deliverables associated with the total effort of the “flipped” team coverage of focused topics. How this will be subdivided will be worked out in class.

5% Final exam

Reminder: Georgia Tech operates on an honor system.

**Weekly Schedule**:

Week 1

Jan 10: Introductory partial meeting of the class.

Assignments for this week (preparation for following week’s class):

Reading:

* 9/11 Commission Report Chapters 1 and 2
* Piore, Adam (2011). “Planning for the Black Swan,” *Scientific American*, vol 304, no 6. Pp. 48-53. A look at nuclear reactor safety and risk management in the context of the Fukushima accident.

Writing:

* Find at least 3 lists of “critical infrastructures” and bring them to class next week. Start by looking at the DHS web site.

Week 2

Jan 17: What we hope to accomplish in this course and how we are going to

do it. Discussion of various kinds of infrastructures and the spectrum of “resilience.”

Assignments for this week:

Reading:

* 9/11 Commission Report Chs 3 and 4

Writing:

* Create a one page ‘personal bio sketch’ (assignment to be discussed in January 17th class session).

Week 3

Jan 24: A discussion of all of the ways critical infrastructures showed up in the events surrounding 9/11. Initial discussion of semester-long projects. Personal bio sketches due.

Assignments for this week:

Reading:

* 9/11 Commission Report Chs 5 and 6

Writing:

* Start to think about an initial plan for asking and trying to answer important questions related to infrastructures and 9/11 (Note: Group assignments to be determined by class during first 3-4 weeks.)

The remainder of the syllabus will be completed after we have had a chance to get to know the participants in our class and determine their interests.