# Outline for Cybersecurity & Behavioral Analytics

# Summer III (covering June and July)

**Schedule:** Wednesdays 6:10 pm – 8:50 pm

**Instructor:** Hasshi Sudler

**Course Objective:**

Many companies that have invested in cybersecurity are realizing that strengthening perimeter defenses is not enough to prevent damaging attacks. Companies are realizing that behavior analytics is critically valuable to predicting how and when attacks may take place. This insightful can guide companies in making timely decisions about how to implement defenses and where to allocate company resources.

This course teaches fundamentals of behavior analytics using statistical predictive models, system dynamics modeling and decision analysis to determine how cyber attackers choose their attack vectors, why victims fail to secure their systems and how network traffic reveals when attacks may be occurring. This course will provide a set of valuable tools to address underlying human behavior in the rapidly evolving cybersecurity field.

**Course expectations:**

Modeling, Statistics

**Course Outline:**

Defining the Attack Surface

Understanding Attack Vectors

Target of attack: Systems, People and Processes

Cyber security frameworks

Strengths and weaknesses of Perimeter defense

Perimeter defense versus behavior analysis

Behavior of Attackers and Victims

Behavior of networks, groups, attacks and responses

Understanding Cyber Attackers

Motivation of Attackers

Target selection

How Attackers select attack vectors

Understanding Victims

Habits of Victims

Why people and companies fail to secure systems

Bounded Rationality

Modeling behavior using System dynamics

Systems Thinking

Causal Loop Diagrams

Modeling behavior using Stock and Flow Models

Determining your Reference Mode

Using Vensim systems modeling tool

Statistical Analysis

Probability of attacks

Probability of reactions

Linear regression and other predictive models

Building predictive models for attacks by industry, company size, and independent variables

Applying behavioral analysis

Causality vs. Correlations

Measuring behavior of networks - detecting when network traffic and access is unusual

Stock and Flow model of attacker motivations

Predicting attacks

Modeling policy changes

Policies are designed to alter behavior - define target behavior

System Dynamics model of current state

System dynamics model of new state

using Stock and flow modeling to measure changes in behavior