Adversarial Thinking Module
National Cybersecurity Curriculum Project
Seth Hamman, Ph.D., Ken Hopkinson, Ph.D.

Overview
This curriculum module provides a basic introduction to adversarial thinking, game theory, and behavioral game theory to help develop cybersecurity students’ abilities to anticipate the strategic actions of cyber adversaries, including where, when, and how they might attack, and their tactics for evading detection. The basic message of the module is that human adversaries are what differentiates cybersecurity from other technical disciplines such as computer science, and, therefore, the concept of adversarial thinking is central to cybersecurity. The goal of the module is to produce enduring strategic-mindedness in students who may otherwise tend to equate cybersecurity with technology-based best practices. This is a stand-alone, self-contained module, with no knowledge prerequisites. The module can be incorporated into virtually any university-level course. A syllabus, learning outcomes, assessment materials, instructor notes, PowerPoint slides, videos, and whole-class interactive exercises are included. This module has been experimentally validated and is the subject of two peer-reviewed journal articles.

Curriculum Package

| Lesson 1: Intro to Adversarial Thinking
| Lesson 2: Intro to Game Theory
| Lesson 3: Intro to Behavioral Game Theory

Materials
- 68 PowerPoint Slides with extensive notes
- Assessment materials with step-by-step solutions
- Custom videos and video clips

3 Lessons of approximately 1 hour each

Adversarial Thinking Learning Outcomes
- Students will be able to analyze a strategic scenario from a game theoretical perspective.
- Students will be able to apply level-k reasoning to derive playing strategies in strategic contests.
- Students will be able to analyze cybersecurity from the strategic perspective of cyber adversaries.

Exercises and Illustrations
- Data Breach – a cyber-themed game used as a pretest-posttest assessment tool to measure the impact of the curriculum module on students’ adversarial thinking abilities (see right panel)
- Illustrating Adversarial Thinking – a profile of the hacker described in Cliff Stoll’s The Cuckoo’s Egg is analyzed for the three components of adversarial thinking
- The Hacker’s Dilemma – a cyber-themed retelling and analysis of the prisoner’s dilemma game
- The Battle of Bismarck Sea – a real-life strategic military situation is analyzed with game theory
- Solomon’s Wise Ruling – game theory is applied to this famous story to try and predict the ending
- The 2/3s Guessing Game – played together in class, this game illustrates the key differences between analytical and behavioral game theory, and the concept of level-k reasoning
- The Hide and Seek Game – a famous experimental game theory game illustrating focal point biases
- The Colonel Blotto Game – a game theoretical model of the scarce resource allocation problem faced in many real-life defense scenarios (see left panel)
- DDoS – a cyber-themed Colonel Blotto game is analyzed using level-k reasoning in multiple dimensions

Recommended Readings
- (many additional books, articles, and websites are cited in the slide notes)

The Data Breach Pretest-Posttest Assessment
This exercise measures students’ adversarial thinking abilities. It tasks them with detecting an employee’s attempt to exfiltrate customer records by strategically allocating log auditing man-hours. The exercise is scored against actual data collected from students cast in the role of the insider threat.

<table>
<thead>
<tr>
<th>Daily Log Files</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value of Data</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Log Auditing Hours (must sum to 100)</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>