2009

Studying Terrorism with Experimental Games

Charles A. Holt
University of Virginia - Main Campus, holt@virginia.edu

Follow this and additional works at: http://research.create.usc.edu/project_summaries

Recommended Citation
http://research.create.usc.edu/project_summaries/41

This Article is brought to you for free and open access by CREATE Research Archive. It has been accepted for inclusion in Research Project Summaries by an authorized administrator of CREATE Research Archive. For more information, please contact gribben@usc.edu.
1. Overview

The goal of this project is to combine insights gleaned from laboratory with a game-theoretic analysis of decisions made by terrorist groups and those charged with defending key assets. Laboratory experiments in economics use financially motivated human subjects. These participants are recruited in groups and are placed in decision-making scenarios, where their cash earnings may depend on strategies they adopt and on decisions of others, as intermediated by random events. Such experimentation is useful in spotting behavioral tendencies that can be used to augment the use and interpretation of formal models of strategic interaction. Terrorism is a prime setting for the use of these experimental techniques, given the high amounts of strategic uncertainty, and the fact that most decision makers operate in settings with somewhat incomplete information about others’ plans and activities. The software developed for the laboratory experiments can also be used for gaming and demonstrations.

The primary focus of year 5 work was the development and testing of software for implementing three attacker/defender games, using the Veconlab platform hosted at the University of Virginia Department of Economics (http://veconlab.econ.virginia.edu/admin.php). To view these games, go to the Games menu and use the three-letter user name: mgn along with the single-letter password: x. These games are the Security Coordination Game, the Attacker-Defender Game, and the Multi-Site Attacker-Defender Game. The software programs for these games combine an administrator interface for setting up the experiment with a user interface for the participants. The administrator component provides options for the number of decision-making rounds, the numbers of participants and their available decision strategies, and the payoff consequences of various combinations of actions and random events. The user component provides instructions that have been configured to match the setup options selected by the administrator, along with screens for selecting decisions, confirming them, and receiving outcome information and earnings results. These experiments are conducted on the web, often with a number of participants located in a computer lab, so the software has to be user friendly and robust to efforts to change decisions or manipulate settings. One of the advantages of experimental methods is replication, or repeated sessions with different groups of participants who interact in multiple rounds. This replication can produce large amounts of decision data, and hence, it is important that the software organize and display data in useful formats for viewing results as they come in and for exporting data to statistical programs for analysis. The Veconlab terrorist game programs under development have all of these features, along with a graphical interface that generates charts as decisions are made and tabulated.

Two of the games, the Security Coordination Game (SCG) and the Attacker Defender Game (AD2), have been fully developed and tested. The Security Coordination Game

"This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001, sub-award number 129561 to the University of Virginia. (GO10805). However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security."
Holt, Studying Terrorism with Experimental Games

(http://veconlab.econ.virginia.edu/scg/scg.php) implements the Kunreuther Heal model of interdependent security games in which security breaches can occur locally or as a result of a cross breach. A defender who invests in local protection can avoid or minimize the chances of a local breach, but still suffer the consequences of a cross breach if other defenders do not invest. The interdependent nature of this game creates a coordination problem that can be mitigated with information about others’ decisions and incentives that change the risk structure of the game. One feature that has been added to this game is a “weakest link” setting in which the degree of protection is determined by the minimum of the various defenders’ levels of security investments.

The second experimental game that has been developed is the Attacker Defender Game (http://veconlab.econ.virginia.edu/ad2/ad2.php) This is a game in which one player either attacks or waits, and the other either goes on high or low alert. The setup allows either neutral or “hot” (attacker-defender) terminology, and either fixed or random matchings of participants. In March, we completed one set of sessions with about 100 subjects using the hot terminology and fixed matchings, which is a more realistic setting. The strategic structure of the game has the property that players need to randomize decisions to avoid losses resulting from being too predictable. The experiment was designed to test the effects of changes in the cost of an attack that could result from added security measures. The experiment involved three attack costs (low, medium, and high) in a setting where the mixed-strategy Nash equilibrium for a single play of the game predicts that the probability of attack is independent of the attack cost. This unintuitive prediction is driven by the fact that defenders go on high alert more often when attack costs are low, and this defender reaction, in equilibrium, offsets any enhanced incentive to attack with lower costs. The data from the experiment, however, do show a sensitivity of attack propensities to attack costs. An analysis of the data that incorporates noise in behavior can be used to generate predictions that fit data averages well. Alternative theoretical explanations include Selten’s “impulse response equilibrium” and some models of learning with limited memory (“stochastic learning equilibrium”). We are in the process of designing experiments to distinguish these alternative explanations.

The third game, the Multi-Site Attacker-Defender Game (http://veconlab.econ.virginia.edu/adn/adn.php) program involves multiple assets (up to 30 sites) that can be defended or attacked, and multiple attackers (up to 5) and defenders (up to 5). When there is more than one attacker, the program permits the option of a chat room between attackers, with each message having a pre-specified probability of being intercepted and read by defenders. The software program offers a lot of flexibility in setting the costs and values of attacks on various assets. Each attacker has one or more “assets” that can be targeted at selected sites. Similarly, each defender has one or more assets that can be located at selected sites. A random defense strategy, with manual override, is also a possible choice. The probability of a successful attack at a given site is an increasing function of the total number of attacker assets targeted to that site, and a decreasing function of the total number of defender assets targeted to that site. The formula can either be ratio based or a logit function with a specified precision parameter. The costs incurred by defenders can depend on the site where defense assets are located, so costs can be site specific if particular sites are harder to defend. These costs are associated with locating an attack asset at a site. In addition, the program permits the specification of a “failed attack cost” that is borne by the attacker who locates an asset at a site where the attack fails. Similarly, attacker costs can also be specified to be site-specific. Attackers may have values for a successful attack that are site specific, and defenders can have site-specific values that are lost if an attack succeeds. These values may not be the same for attackers and defenders, for example, if a given site has more symbolic value for one player type than the other. When an attack fails, defenders may or may not observe this, depending on how the “near miss view probability” parameter is set.
The strategic structure of the resulting games has two important game-theoretic dimensions. There is a coordination problem for players of the same type, since attacks are more likely to succeed if they are concentrated. And the success formula may be such that defenders need to coordinate defenses so as to avoid holes in coverage. There is also a guessing game dimension, which is a generalization of the simple matching-pennies game for two players with two decisions. As with matching pennies, players in the multi-site game have an incentive to guess correctly where the players of the other type will concentrate their assets; attackers want to avoid (“miss-match”) defense concentrations, and defenders want to match attack concentrations. This combination of the strategy of the coordination and matching-pennies games makes this a rich game, and the setup options permit a rich variety of information structures in terms of message intercepts and near-miss views. This program is currently being tested in the laboratory, and several projects are planned for the spring.

2. Research Accomplishments

2.1. An Experimental Analysis of Attacker/Defender Games (Charles Holt, Ricky Sahu, and Angela Smith)

Abstract: This paper reports results of two-person games in which the defender chooses between high or low alert states, and the attacker chooses whether to attack or wait. High alerts and attacks are costly. Low alerts and attacks are risky in the sense that successful attacks are especially costly to the defender and failed attacks are especially costly to the attacker. The effects of policies that alter the attack cost to the attacker are examined in comparison with game-theoretic predictions. In a Nash equilibrium, the probability of attack is invariant to changes in attack costs, but a positive correlation is present in the data for an experiment conducted with fixed matchings and payoffs that are presented in terms of the costs and benefits derived from the attacker/defender context. The empirical analysis is focused on learning and strategic anticipations.

3. Applied Relevance

Even though game theory provides a well-structured apparatus for studying strategic decisions made by highly motivated players, the behavioral relevance of these theories can be evaluated with laboratory experiments, using insights from behavioral psychology.

4. Collaborative Projects

I have communicated with Catherine Eckel, Rachel Croson, and Dan Arce at the University of Texas-Dallas, who are also beginning work on experimentation in terrorism-related topics. Rachel Croson was a participant in the August 2008 conference at CREATE.

The initial experiments done with the Attacker Defender game were run in collaboration with Professor Angela Smith, from James Madison University. Research assistance was provided by Ricky Sahu, a student at the University of Virginia.

5. Research Products

| Research Products (Please detail below) | # |
5.1. Publications and Reports


5.2. Presentations

No presentations have been made.

5.3. Models, Databases, and Software Tools and Products

The Security Coordination Game and the Attacker Defender Game have been completed and are hosted on the Veconlab web site under the games menu: [http://veconlab.econ.virginia.edu/games.php](http://veconlab.econ.virginia.edu/games.php). Each program consists of about 25 PHP scripts and an associated database. These are non-commercial products for use in research experiments, and for educational demonstrations. A second program, with a more complex setting involving multiple assets to be defended or attacked, is under development.

6. Education and Outreach Products

<table>
<thead>
<tr>
<th>Education and Outreach Initiatives (Please detail below)</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td># of students supported (funded by CREATE)</td>
<td>1</td>
</tr>
<tr>
<td># of students involved (funded by CREATE + any other programs)</td>
<td>0</td>
</tr>
<tr>
<td># of students graduated</td>
<td>0</td>
</tr>
<tr>
<td># of contacts with DHS, other Federal agencies, or State/Local (committees)</td>
<td>0</td>
</tr>
<tr>
<td># of existing courses modified with new material</td>
<td>1</td>
</tr>
<tr>
<td># of new courses developed</td>
<td>0</td>
</tr>
<tr>
<td># of new certificate programs developed</td>
<td>0</td>
</tr>
<tr>
<td># of new degree programs developed</td>
<td>0</td>
</tr>
</tbody>
</table>

Research assistance for the March 2009 Attacker Defender experiment was provided by Ricky Sahu, a 4th year student at the University of Virginia, who graduated in May 2009. The Security Coordination Game software has been used in ECON 482 (Experimental Economics) at the University of Virginia to illustrate solutions to the coordination problem created by interdependent security decisions.