Security is a global concern. A fundamental challenge of protecting critical infrastructure (for example, ports, airports) as well as critical resources (for example, fisheries, wildlife) arises from limited availability of security resources. Protecting all targets at all times is typically not realistic, and as a result, 100 percent security is not possible. Instead, security resources must be deployed intelligently, an endeavor in which artificial intelligence (AI) can play a major role.

In recent years, AI-based applications have increasingly been used in real-world domains. For example, game theory–based decision aids have been successfully deployed in various security settings to protect ports, airports, and wildlife. This article describes our unique problem-to-project educational approach that used games rooted in real-world issues to teach AI concepts to diverse audiences. Specifically, our educational program began by presenting real-world security issues, and progressively introduced complex AI concepts using lectures, interactive exercises, and ultimately hands-on games to promote learning. We describe our experience in applying this approach to several audiences, including students of an urban public high school, university undergraduates, and security domain experts who protect wildlife. We evaluated our approach based on results from the games and participant surveys.
Security Games: Using AI to Address Real-World Problems

In recent years, the field of security games, a subfield of AI, has drawn increasing attention from outside the AI community (Tambe 2011). In particular, game theory–based decision aids have been successfully deployed to protect critical infrastructure such as airports and ports (for example, Pita et al. [2008]), making real-world impacts and resulting in fundamental changes to security operations for various organizations. Security problems continue to evolve worldwide, creating new research challenges and practical applications for security games. Focusing on wildlife protection specifically, poaching represents the second largest threat to biodiversity after habitat destruction. This led to the development of green security games, a subfield of security games focused on protecting forests (Johnson, Fang, and Tambe 2012), fisheries (Haskell et al. 2014) and wildlife (Fang, Stone, and Tambe 2015; Kar et al. 2016). Although park rangers conduct patrols to combat poaching, security resources are often limited in vast conservation areas. Manually generating patrol schedules can require considerable effort from wildlife security staff, and such manual plans can be predictable, allowing poachers to exploit patrol schedules. Our security game–based solutions combine different AI subfields—including game theory, optimization, and machine learning—to help rangers automatically generate randomized patrol strategies that account for models of poachers’ behaviors.

As a subfield of computational game theory, security games (Tambe 2011) model the strategic interaction between two players: a defender and an adversary. Security games take into account: (1) differences in the importance of targets; (2) the responses of attacker (for example, poacher) behavior to the security posture; and (3) potential uncertainty over the types, capabilities, knowledge, and priorities of attackers. This problem can be cast as a game. As a brief example, a security game in the wildlife domain involves the following: the ranger allocates security resources (that is, ranger patrol teams) to protect a set of critical targets of varying importance (figure 1). Higher value targets may be portions of a protected area with higher biodiversity, larger numbers of animals, and/or protected species. The ranger deploys a mixed strategy, which optimizes over all possible configurations of allocating patrols across these targets, and is represented as a vector of probabilities of covering any given target. The poacher conducts surveillance on the ranger’s strategy before selecting a target to attack, with the goal of maximizing payoff for any given defender strategy. The players’ actions lead to different payoff values, and the defender’s performance is evaluated by her or his expected utility. The defender’s goal is to find the optimal strategy so as to maximize expected utility, knowing she or he faces an adaptive adversary who will respond to any deployed strategy.

Prior Work: Teaching with Projects, Problems, and Scaffolds

The potential applications of this work to various contexts have created the need to introduce the AI concepts underlying security games to individuals with limited AI backgrounds. These include not only students, but also audiences outside of traditional classroom settings. Given recent advances in green security games in particular, helping decision makers and those who may consider using AI-based decision aids in the field to understand the underlying theoretical framework can aid in fostering adoption of these emerging technologies.

Teaching security games and related concepts such as probability, optimization, and agent-based modeling to those with limited AI backgrounds can be challenging. In traditional classroom settings, AI concepts have been made accessible to undergraduate students who enter with limited AI backgrounds (Stern and Sterling 1996, Parsons and Sklar 2004, Wollowski 2014). One method that has been effective in teaching AI in classrooms is the use of games. For instance, games have been used to teach robotics, (Wong, Zink, and Koenig 2010), Pac-Man has been used as a tool to teach various AI concepts (DeNero and Klein 2010), and in a game called CyberCIEGE, players build a virtual world while learning about AI issues involved in cyber security (Cone et al. 2007). However, no prior work describes effective methods for teaching AI to audiences beyond the classroom. Similarly, little evidence speaks to approaches for framing such games to teach and foster interest in AI.

We explored the possibility of using real-world problems to frame AI instruction. This approach is similar to project-based learning, an educational framework that aims to increase motivation for learning by engaging students in investigation (Blumenfield et al. 1991). Specifically, project-based learning involves presenting a problem that guides activities, and such activities culminate in a final product to answer the initial question. A meta-analysis of project-based learning studies conducted in real-world classrooms found that such an approach results in positive effect on application of general science knowledge, and although no immediate main effect on declarative knowledge (of underlying concepts, facts) was found, this increased over time (Dochy et al. 2003). Similar approaches have been applied to engineering curricula at the college level at several higher education institutions, and although no systematic evaluation results could be identified, qualitative feedback from students indicated that they evaluated the approach positively (Mills and Treagust 2003). Particularly relevant to AI, Gini et al. (1997) used a variety of robotics projects to teach robotics and other AI concepts at the college level; however,
no evaluation results were provided. In sum, project-based learning has shown promise in piquing student interest and improving application of knowledge in general, but its effectiveness as a technique for teaching AI specifically, particularly outside of the classroom, has not yet been investigated.

Project-based learning also lends itself well to other instructional strategies. For instance, scaffolding is an instructional framework that can help learners achieve learning goals in an assisted, often stepwise manner (Wood, Bruner, and Ross 1976). Broadly, in instructional scaffolding, teachers provide adjustable support for learners to enhance learning and promote progressive mastery of material by introducing new concepts and skills in a systematic manner (Pea 2004). Within a scaffolding framework, imaginary problems have been used to highlight the larger importance of learning goals, followed by project-based learning, which can serve to structure specific learning activities and tasks (Barron et al. 1998). Such a “problem-to-project” scaffolding approach has previously been found to improve a variety of classroom learning outcomes (Barron et al. 1998). However, we could find no evidence speaking to its efficacy for teaching AI specifically, or for teaching outside of traditional classroom settings.

Real-World Problem-to-Project Teaching Approach

Building on our prior paper (Sintov et al. 2016), this article describes our teaching approach, which used a problem-to-project scaffolding framework. The program began by presenting real-world wildlife security problems that painted a broad picture for why learning security game and other AI concepts is important. As detailed in the following sections, we then used project-based learning techniques along with instructional support to introduce progressively complex AI concepts underlying security games, including probabilistic reasoning, optimization, and agent-based modeling. We taught these concepts with a combination of lectures, interactive exercises, and hands-on games to help learners tie learning activities to the larger real-world security goals. We describe our experiences delivering this approach to several audiences, including: (1) students of an urban public high school; (2) undergraduate students at a large private university; and (3) law enforcement officers and rangers who protect wildlife in Indonesia. It is important to note that although the wildlife security problems used in our program are based on real-world data and input from security experts working...
in the field on such problems, they represent an abstracted version of the problems they aim to address.

We evaluate our teaching approach in several ways: (1) we show how high school and university participants played the games and the effectiveness of their strategies playing as defender, represented as defender utility, that is, the defender's overall payoff obtained when peers play as poachers; (2) we show how security experts who typically generate defender strategies in the real world played as poachers against an AI algorithm-generated defender strategy; and (3) we assess participants' perceptions of our approach using surveys. We make recommendations for teaching similar topics to audiences with limited AI backgrounds.

Our Ranger Versus Poacher Games

We used interactive games as a key teaching tool in our program. Prior to playing these games, learners participated in lectures, discussions, and other learning activities. The games therefore provided learners an opportunity to apply their culmination of knowledge, while also allowing them to build on this knowledge through hands-on exercises that allowed trial-and-error testing of their ideas.

Adapting an online computer game used in another study of green security games (Kar et al. 2016), we created a board game. As background information, we describe the computer game here.

The computer game was set in a protected wildlife park that was divided into a 5-by-5 grid, yielding 25 distinct cells, with hippopotami and rangers scattered throughout (figure 1). In the computer game, participants played the role of a poacher whose objective was to hunt as many hippopotami as possible while avoiding detection by rangers. Participants were primed by reading a background story detailing the hardships of a poacher's life as well as the rewards of successful poaching. They could navigate throughout the park and select any cell to "attack." They were asked to consider three main criteria in deciding where to attack: distance, animal density, and coverage probability. Distance was the distance from the starting position to the attack location. This was incorporated to better approximate the real-world scenario whereby time and distance traveled to locate a snare represents a cost to poachers. Animal density was represented by hippopotamus density, which varied across the park, but density in a particular region (cell) did not change within a given round. Coverage probability was represented by a heat map overlaid on the park, indicating the likelihood of ranger presence at a given cell. Cells with higher coverage probabilities were more red, whereas those with lower coverage probabilities were more green. This represents the real-world surveillance situation in which poachers have knowledge of general patterns of ranger locations, but cannot always predict exact ranger presence.

In the computer game, a computer algorithm determined ranger locations. A total of nine rangers were protecting the park, with each ranger protecting one cell. Therefore, only 9 of 25 distinct cells in the park were actually protected, and the color-shaded heat map showed players only the probability of ranger presence at each cell. Additionally, the following detailed information was available by clicking on any cell: monetary reward for poaching successfully, monetary penalty for getting caught, and chance of success/failure (figure 1). Players were successful in the game if they attacked a cell without a ranger and failed if a ranger was protecting their chosen cell.

For our teaching program, we adapted this computer game into a board game (figure 2) to provide learners the opportunity to play as both poachers and rangers. Board games used the same background story, 5-by-5 grid, defender resource allocation, and reward distribution as the computer game. However, instead of using the Queen Elizabeth National Park map and images of hippopotami to show the relative “value” of different areas, the board games used movable figures to represent animal distributions. This did not require any equipment such as computers, making it easily scalable to other settings. Also, in board games, learners could take turns playing the roles of ranger and poacher, whereas the computer game permitted play only as poachers. Additionally, the board games facilitated peer interaction. One group, acting as defender, was given a limited number of defense resources. They could place ranger figures anywhere on the board to generate the defender strategy. The other group, acting as adversary, placed the poacher figure anywhere on the board in deciding where to “poach” against their peers’ defender strategy, representing poaching decision making.

Finally, the board game did not provide immediate feedback on probabilities and rewards associated with success or failure (right-hand panel of figure 1), better approximating the real-world situation in which this level of detail is typically unavailable. Therefore, the board games were leveraged as a more scalable and flexible learning tool. Although we aimed to abstract the real-world problem to the extent possible in this game, not all details of the real-world scenario could be included, and hence findings should be viewed in light of this limitation.

High School Students

An AI unit focused on computational game theory was delivered to a group of high school students as the last unit of study in a year-long engineering elective course. An underlying tenet of the unit was that AI concepts can be made accessible to anyone. We reasoned that AI concepts could also provide a great launching point into a discussion on computers in
general; if students could understand quantitative decision making in this context, they could use it as a base of knowledge from which other computer science concepts could be more readily understood. Unit objectives included students gaining probabilistic reasoning skills, enhancing student interest in AI, and high levels of student satisfaction with the learning experience. The unit was developed during summer 2014, funded by the National Science Foundation’s Research Experience for Teachers program called ACCESS 4Teachers, and was based on an undergraduate-level course at the University of Southern California titled CS499: Artificial Intelligence and Science Fiction (Tambe, Balsamo, and Bowring 2008).

Participants

The 30 students who participated in the elective course were juniors and seniors at an urban public charter high school located in Los Angeles. All students were of Hispanic or African-American origin, resided in South Los Angeles, and the majority qualified for free or reduced price lunch. Based on a subset of students who responded to our feedback survey, the mean age of the group was 18.1 years and roughly 36 percent were female.

Unit Structure

The unit began with a basic exploration of the nature of human intelligence and how machines (both fictional and real) have been made to mimic human nature. Consistent with a scaffolding framework, we next placed an emphasis on thinking about problems from a quantitative perspective, and considering how humanlike qualities (emotions, risk-aversion, and others) could be quantified to enable computers to act in an intelligent fashion. To illustrate these ideas, students read stories from Asimov’s *I, Robot* and *Robot Visions*, watched clips of the character Data from *Star Trek*, and debated the meaning of intelligence based on these stories. Students tended to be very engaged in these real-world examples, and were often perplexed when they saw how quantitatively-based decisions differed from their emotional ones. Next, to review the concept of probability, more pop-culture examples were given, ranging from an exploration of the California Lottery to the popular game show *Deal or No Deal?*, and the unit progressed to introducing...
the concept of expected value. The teacher delivered lectures, and skills were reinforced by students completing worksheets and applied problems. For many students, a full grasp of the material required a review of fraction operations, which were reviewed on an ad hoc basis in small groups. The unit culminated with students integrating and applying their knowledge to play the games.

Final Project
The final project for the unit used the board game described previously (figure 2). To reinforce the idea of quantitative decision making, students were tasked with designing their own defender strategies using short formulas to allocate a limited number of ranger-hours to the 25 grid cells in the game. Students worked independently or in groups to complete the strategies (in this case, using Google spreadsheets). These spreadsheets were then used to generate 12 distinct games based on the student-designed defense strategies. Taking on the role of poacher, students played the games against defender strategies generated by other groups. Finally, students reviewed the results of their strategies, made adjustments, and presented their work to explain where initial strategies were particularly successful or unsuccessful.

Results of Games
Different groups employed different methods in designing defender strategies. While some chose to concentrate ranger patrols in areas dense with animals, often associated with a high probability of failure, others developed strategies in which the expected value for poachers was nearly zero. Figure 3 shows the expected defender utilities obtained by each of the 12 student groups based on the attacks conducted on the other teams’ defender strategies. The team with the highest expected utility generated a strategy that not only considered the animal densities, but also the distance from the poacher’s starting location, placing lower coverage in cells farther away from the poacher’s starting location. The team with the lowest expected utility placed maximum coverage (100 percent) on the highest animal density cell and divided remaining resources (ranger-hours) uniformly across all remaining targets, ignoring important factors like animal distribution and distance.

Feedback
A total of 14 (8 males, 5 females, 1 declining to state) out of 30 students responded to a survey that assessed their experiences in the unit. To inform unit objectives, questions assessed the unit’s impact on learners’ overall interest in AI, perceived educational value of the unit, and likelihood of recommending the unit to others. Responses were provided on Likert scales (for example, ranging from 1 = strongly disagree to 7 = strongly agree). Open-ended questions assessed general likes and dislikes. More than 70 percent of respondents agreed (somewhat or more) that the activity increased their interest in AI, and 93 percent agreed (somewhat or more) that the activity was a valuable learning experience. Additionally, more than 90 percent responded that they would recommend the unit to other high school students. Open-ended responses indicated that respondents particularly enjoyed the interactive game aspect of the course. The least enjoyable aspects of the course were those that students perceived as tedious or repetitive, such as calculating probabilities.
University Students

AI and security games were introduced to a class of University of Southern California (USC) freshmen as a two-week unit in their Freshman Academy course in fall 2015, which is an introductory engineering course aimed at introducing students to ongoing research at USC across various engineering disciplines. Similar to the high school course described in the previous section, the two-week AI unit portion of the course was also designed based on a seminar at USC titled CS499: Artificial Intelligence and Science Fiction. Aligning with unit objectives for the high schools students, objectives for the university students included honing probabilistic reasoning skills, enhancing student interest in AI, and high levels of student satisfaction with the learning experience.

Participants

The 30 students who took part in the AI unit were all USC freshmen majoring in engineering. Based on a subset of students who responded to our feedback survey, the mean age of the group was 18.2 years, and roughly 77 percent were female.

Unit Structure

Instructors opened the unit by introducing security as a global concern, and highlighted problems specific to wildlife security. Step by step, the unit introduced more complex concepts, starting with basic concepts in AI and game theory. As part of our scaffolding framework, to teach the notion of payoffs in a game context, the classic prisoner’s dilemma problem in game theory was introduced. Discussion was facilitated around this topic to provide foundational understanding regarding payoffs in the games (that is, animal densities and penalties). Faculty and CEOs of technical startups then facilitated discussion around the use of AI applications to solve real-world security problems, painting a picture of the various ways in which AI can influence day-to-day life. Similar to the high school students, the unit culminated with students integrating and applying their knowledge to play the games. Basic game-theoretic concepts such as maximin were explained to help students focus on subsets of information in decision making: for instance, in the case of maximin, when only information about the payoffs in the game is available, instructors aimed to help students design the most conservative strategy.

Final Project

Similar to the final project for high school students described above, following the lecture and discussion-based elements of the unit, students played the board game. Here, students first played as rangers. The class was divided into seven groups, each of which designed its own defender strategy on a game board. Some groups chose to allocate ranger coverage in proportion to the number of animals, whereas others placed highest coverage at the highest animal density region and uniformly everywhere else; some others developed strategies in which the expected value for poachers was nearly zero across all of the regions of the park. Each group’s strategy was then shown to the other groups, who played the game in the poacher role against their peers’ defender strategies.

Results of Games

The resulting defender utilities for each university student group playing the board games is shown in figure 4. The team with the lowest defender utility (G3) placed very low coverage (< 0.40) in the highest
animal density cell and as expected, all the other teams attacked that cell. Similar results were obtained for group G7, which placed a coverage of 0.50 on the highest animal density target. Other teams performed reasonably well but none performed better than maximin, which would have resulted in a defender expected utility of –2.17.

Comparing the university students’ results with those of the high school students (figure 3), visual inspection suggests that overall, the high school students outperformed the university students. This may be due to the limited time allotted to the university students. The high school students had more time, which allowed more discussion and scrutinizing over decisions. However, the small sample sizes prohibited statistical comparison, so this observation should be interpreted with caution.

Feedback
A total of 24 (7 males and 17 females) out of 30 university students responded to a survey that assessed their experiences in the unit. Questions mirrored those administered to the high school students to address unit objectives. More than 69 percent of respondents indicated that the activity increased their interest in AI at least somewhat, and more than 80 percent agreed (somewhat or more) that the activity was a valuable learning experience. Additionally, more than 65 percent responded that they would recommend the activity to peers. Qualitative data suggested that respondents particularly enjoyed the interactive aspects of the unit. The least enjoyable aspects of the unit were cases in which students in a team couldn’t agree on a particular strategy.

Security Experts
A three-day workshop was developed in collaboration with the World Wildlife Fund (WWF) to demonstrate the value of AI-based solutions for security to security experts who protect wildlife. The workshop was held in Bandar Lampung, Sumatra, Indonesia, in May 2015. A game theory–based decision aid called PAWS (Yang et al. [2014]; Protection Assistant for Wildlife Security) was developed, in part, based on a study of green security games for the purpose of protecting wildlife from poaching. We sought to teach how AI systems like PAWS fed with partial information can generate patrol strategies that can perform relative to strategies created by field experts with extensive knowledge of the system. Hence, diverging a bit from the classroom-based units described above, our objectives for this third audience included promoting participant adoption of AI-based software (that is, PAWS), sharpening participants’ probabilistic reasoning skills especially in the poacher role, and participant satisfaction with the learning experience.

Participants
A total of 28 participants (26 males and 2 females) attended the workshop. They represented the five primary groups (either government or NGO) involved in protecting wildlife in Bukit Barisan Selatan and Tesso Nilo national parks on Sumatra: the Indonesian National Park Service, WWF, Wildlife Conservation Society, Indonesian Rhino Foundation, and prosecution officers from the court. The majority of these individuals were rangers with a great deal of domain expertise in wildlife crime and protection who directly conduct field patrols over conservation areas; the prosecutors report cases to lawyers and judges who can open official investigations to prosecute wildlife crime. The mean age of the sample was 35.0 years (SD = 7.5), and mean years of formal schooling was 14.0 (SD = 3.1). Approximately 60 percent of respondents identified their job sector as wildlife/national park protection, 20 percent as nonprofit/NGO, and 20 percent as law enforcement, and overall they had an average of 9.6 years of experience working in wildlife protection (SD = 6.1).

Participants were native speakers of Bahasa Indonesia. The instructors delivered the workshop in English and interpreters translated all the material between instructors and participants throughout the three-day course. All written materials were made available in both English and Bahasa Indonesia.

Unit Structure
We began by introducing basic examples and theoretical foundations relevant to agent-based modeling, game theory, and security games through lectures. Building on and integrating this knowledge as part of our scaffolding framework, we next presented applications that leverage multiple AI techniques. Learners also discussed in groups various challenges faced in wildlife protection and solutions for those challenges, including AI-based solutions. They played the computer-based game as poachers. On the last day, they had the opportunity to integrate and apply their knowledge in playing the board game as poachers and rangers. They also reflected on their results and shared ideas for improving patrolling effectiveness. These interactive exercises provided learners with a new lens for understanding poachers’ behaviors and limits of manual patrolling strategies, as well as introducing the methodology and advantages of game-theoretic solutions.

Security Game Tutorials
On the first day of the workshop, we introduced security game examples from several domains, beginning with a basic security game. We explained how the defender could optimally conduct patrols over targets and how attackers may respond against that strategy. We next covered (1) real-world applications of security games for protecting critical infrastructure and (2) challenges in wildlife protection and the applica-
tion of security games to this domain specifically, reviewing how adversaries’ behaviors are modeled and how to optimize patrolling strategies through allocating limited security resources. Finally, we presented our PAWS software—which was built based on security game models for addressing wildlife protection problems—describing data inputs (for example, animal density, poaching data) and what outputs are generated (for example, models of poachers’ behaviors and suggested patrolling routes for rangers). We described how similar approaches had been previously successfully used in the wildlife domain, and how they could be used on Sumatra with PAWS.

Discussion Sessions
Participants engaged in several discussion sessions on challenges in wildlife protection including resources (that is, factors that motivate people to enter protected areas), illegal activities (that is, types of illegal activities in conservation areas), and wildlife protection (that is, improving security approaches). In small groups, they exchanged knowledge about these topics and generated potential solutions; each group then presented their conclusions to the rest of the groups. We encouraged groups to develop solutions and provide feedback that could be conceptualized in a game-theoretic manner and potentially incorporated into AI software.

Games
Participants played the board game as poachers and rangers. For this activity, participants were divided into two groups. Each group took turns playing as rangers (who created patrol strategies) and poachers (who decided where to poach in games generated by the other team), and each defender strategy was played only once.

Given the large amount of time for the workshop relative to the classroom-based units, in addition to board games, every participant played five rounds of the computer-based games as poachers (figure 5). After each round, the poacher behavior models were updated based on participants’ responses, and each subsequent game used a defender strategy created using these updated models. On the final day, we presented the game results, that is, the defender utilities based on poachers’ decisions in the online games.

By playing these games in a repeated fashion, the participants developed a better understanding of how poachers may react to rangers’ strategies over time, and of the weaknesses of various defender strategies. They also learned how AI software such as PAWS can make optimal decisions based on models of players’ behaviors, and how such decisions can adapt and improve over time as more data are collected.

Results of Games
Each defender strategy in the board games was played only once, so the results based on single data points may not be reliable. In light of this and the fact that only the security experts played the computer game (whereas high school and university students did not), we highlight the results of the computer games here. Figure 6 shows the defender utilities obtained by deploying AI-based defender strategies (that is, PAWS) over several rounds against security experts playing as poachers. In the figure, lower values on the y-axis indicate better participant performance, and worse performance by PAWS. We observe that PAWS’s performance begins low, initially increases, then declines. This suggests some improvement and learning over time among the security experts, providing modest support of our unit objective of improving probabilistic reasoning skills.
Feedback

A survey administered at the end of the unit addressed unit objectives. Approximately 79 percent of learners were at least somewhat willing to adopt PAWS (mean = 5.9 on a scale of 1 [strongly disagree] – 7 [strongly agree], SD = 1.1). Additionally, open-ended responses also largely supported the purpose of the PAWS software. Roughly half of respondents (n = 15) commented that PAWS could optimize patrols and would make the job of patrolling easier. When asked about software limitations, respondents recommended increasing complexity of models, including approximately one-third (n = 10) of respondents suggesting that dynamic animal distribution models be added. This latter point highlights the challenges faced by AI researchers in accurately representing all details of a given real-world scenario.

Regarding satisfaction with the unit, 86 percent rating the learning experience as at least somewhat useful (mean = 5.7 on a scale of 1 [completely useless] – 7 [extremely useful], SD = 0.8), and more than 96 percent of respondents rated it as at least somewhat important (mean = 6.0 on a scale of 1 [extremely unimportant] – 7 [extremely important], SD = 1.0). Additionally, more than 86 percent of respondents reported that they were at least somewhat likely to recommend it to peers (mean = 6.04 on a scale of 1 [strongly disagree] – 7 [strongly agree], SD = 1.04).

Conclusion

This article describes our unique approach that used a real-world problem-to-project scaffolding framework to teach game-theoretic concepts to several audiences. Learners included students at an urban public high school, university undergraduate students, and law enforcement officers and park rangers who protect wildlife in Indonesia. Our instructional units began by presenting real-world problems in wildlife and other security domains that painted the broad picture for why learning security game concepts is important. Throughout the learning units, techniques from project-based learning along with instructional support were used to progressively introduce complex AI concepts and help learners tie learning activities to the larger real-world security goals. Games were a key learning tool in our approach. Members of all three audiences played the role of two different actors as part of our games: (1) playing as rangers, they generated defender strategies to protect against poachers’ attacks; (2) as poachers, they attempted to outsmart the defender strategies generated by their peers to earn the highest possible rewards. This approach not only gave learners valuable hands-on experience with complex AI concepts, but also in the development of real-world applications for security.

Participant feedback was consistently positive, with the majority of participants from all three audiences rating the learning experiences as useful, and
indicated they would recommend the unit to others. In addition, the majority of the high school and university students reported that it increased their interest in AI. These results are particularly notable given the wide age range and cultural backgrounds of participants, and suggests that our approach was broadly accessible and engaging.

The benefits of problem-to-project scaffolding in our work included having a unifying theme, enabling both learners and instructors to tie concepts and tasks back to a central idea. A related benefit was that the theme afforded the ability to enhance relevance, especially for audiences outside of the classroom, highlighting the value of our approach for teaching concepts in AI to learners representing a broad swath of age, gender, and cultural backgrounds. Additionally, learners showed relatively high levels of engagement, as evidenced by survey findings and qualitative feedback. Being able to meet students where they were at, and serve different learning styles using a variety of activities, was another benefit of the broader scaffolding approach. Drawbacks of our scaffolding framework included somewhat of a narrow focus: by beginning with a particular security problem, a circumscribed range of AI topics fit with the unit. This also led to development of instructional materials specific to the problem.

These findings suggest that our approach may potentially be applied successfully to additional audiences. For instance, our approach can help address educators’ needs, as a recent study found that many are seeking more cutting-edge classroom materials (Wollowski et al. 2015). A possible additional target group is security organizations that could benefit from security applications based on AI and game theory. Enhancing decision makers’ and field officers’ understanding of the theory on which these applications are based could foster the adoption of emerging AI-based decision aids.

Limitations and Future Directions
Our findings should be viewed in light of several limitations. First, it is important to note that although the wildlife security problems used in our program were based on real-world data and input from security experts working in the field on such problems, they represent an abstracted version of the problems they aim to address. In addition, it is unclear how our approach would generalize to teaching AI topics beyond game theory and security games. In the future, we plan to adapt our activities to focus on other AI topics. We also plan to incorporate new activities; for instance, an activity for learners to analyze defender strategies in depth, bringing to light subtle human biases that may affect initial strategies, thereby highlighting benefits of AI agents (compared to humans) in decision making.

Acknowledgements
This work was supported by MURI Grant W911NF-11-1-03 and World Wildlife Fund PAWS Anti-Poaching Grant. The authors would like to thank Job Charles, Rois Mahmud, and Citra Ayu Wardani for their integral roles in planning and implementing the workshop. We also thank Sarine Aratoon, Jori Barash, and Elliott Wezerek for their help with preparing the data.

References
Parsons, S., and Sklar, E. 2004. Teaching AI Using LEGO Mindstorms. In Accessible Hands-on AI and Robotics Educa-
Debarun Kar is a fourth year PhD student in the Computer Science department at the University of Southern California. He is working with Milind Tambe in the Teamcore Research group. His current research is in the field of artificial intelligence and multiagent systems, focusing on computational game theory with applications to security and sustainability domains. On the subject of security games he has coauthored papers that have been presented at AAMAS and AAAI conferences, in both the main track and the industry track. He has also organized workshops on the topic of security games at AAMAS. He received his M.S. degree from the Indian Institute of Technology Madras in India, where he was nominated for the Biswajit Sain memorial award for best M.S. thesis in 2014. His M.S. thesis focused on feature weighting and confidence augmented predictions for real-world case-based reasoning systems.

Thanh Nguyen is a postdoctoral researcher at the University of Michigan. She completed her PhD in computer science at the University of Southern California (USC) in 2016. While at USC, she was a member of the Teamcore research lab where the whole idea of security games was conceived and developed. Her work is motivated by real-world security problems, ranging from domains in infrastructure security (for example, the protection of ports and airports from terrorists) to green security (for example, protecting forests and wildlife from smugglers and poachers) and cyber security (for example, protecting computer networks from botnets). Thanh has published extensively in several leading conferences in AI. She has contributed to building real-world security applications, including the PAWS application for a conservation area in Southeast Asia for protecting tigers and the CAPTURE application for the Queen Elizabeth National Park in Uganda for protecting wildlife.

Fei Fang is a postdoctoral fellow at the Center for Research on Computation and Society (CRCS), Harvard University, and an adjunct assistant professor at the Institute for Software Research at Carnegie Mellon University. She received her Ph.D. from the Department of Computer Science at the University of Southern California in June 2016. She received her bachelor degree from the Department of Electronic Engineering, Tsinghua University in July 2011. Her research lies in the field of artificial intelligence and multiagent systems, focusing on computational game theory with applications to security and sustainability domains. Her work has won the Deployed Application Award at Innovative Applications of Artificial Intelligence (IAAI’16) and the outstanding paper award in the Computational Sustainability track at the International Joint Conferences on Artificial Intelligence (IJCAI’15).

Nicole Sintov is an assistant professor of behavior, decision making, and sustainability at the Ohio State University's School of Environment and Natural Resources. At the time this article was written, she was an assistant professor of research at the Price School of Public Policy and research lead at the Information Sciences Institute at the University of Southern California (USC). As an environmental psychologist, her research focuses on developing and evaluating strategies to change human behavior pertaining to sustainability issues (for example, energy and water consumption), and understanding processes of behavior change. Using a highly interdisciplinary approach, her research program integrates the development, application, and dissemination of sustainable innovations. She has published widely on the interface between humans and power systems, with publications in Energy Policy, International Journal for Sustainability in Higher Education, and Journal of Energy & Buildings.


Kevin Hoffman is the blended learning analyst at Aspire Public Schools in Oakland, CA. In this role, he works to support the use and review the efficacy of technology-aided instruction in more than 20 public charter schools serving students in grades K–12 in California’s Los Angeles, Central Valley, and Bay Area regions. Previously, he taught multiple levels of mathematics and engineering at Alliance Health Services Academy, a public charter high school in South Los Angeles. While in this role, he spent a summer in Milind Tambe’s Teamcore research lab as a fellow participating in the NSF-funded University of Southern California ACCESS 4Teachers RET program, which led to his implementing a unit of instruction on artificial intelligence for his advanced engineering class. He is passionate about how technology can be leveraged in high-need classrooms to create equitable opportunities for students of all backgrounds.

Arnaud Lyet works at World Wildlife Fund as a conservation scientist. He focuses on analysis and management of animal populations and is especially interested in the monitoring and conservation of rare, elusive, and threatened large mammal species. His monitoring and conservation approach is based on an integrated use of spatial distribution modeling, large-scale censuses methods accounting for imperfect detection of animals, and multistate capture–recapture methods.

Milind Tambe is founding codirector of CAIS, the University of Southern California Center for AI in Society, and Helen N. and Emmett H. Jones professor in engineering at the University of Southern California Center for AI in Society, and Helen N. and Emmett H. Jones professor in engineering at the University of Southern California. He is a fellow of AAAI and ACM, as well as recipient of the ACM/SIGART Autonomous Agents Research Award, Christopher Columbus Fellowship Foundation Homeland security award, INFORMS Wagner prize for excellence in operations research practice, Rist Prize of the Military Operations Research Society, RoboCup Scientific Challenge Award, and others. Tambe’s pioneering real-world deployments of security games have led him and his team to receive the US Coast Guard Meritorious Team Commendation from the commandant, US Coast Guard First District’s Operational Excellence Award, certificate of appreciation from the US Federal Air Marshals Service, and special commendation given by LA Airport police from the city of Los Angeles. He has also cofounded a company based on his research, Avatar Intelligence, where he serves as the director of research.