"This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Cooperative Agreement No. 2010-ST-061-RE0001. 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 or the University of Southern California."

Cooperative Agreement No. 2010-ST-061-RE0001
Department of Homeland Security

September 22, 2012
ABOUT CREATE

The National Center for Risk and Economic Analysis of Terrorism Events (CREATE) was the first university-based Center of Excellence (COE) funded by University Programs of the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). CREATE started operations in March of 2004. This annual report covers the seventh year of CREATE funding from October 2011 to August 2012, under Cooperative Agreement 2010-ST-061-RE0001 from DHS. While the text of this report focuses on the seventh year, all data tables, publications, lists of participants, students, and presentations and events are cumulative from the inception of CREATE.

CREATE’s research mission is to develop advanced models and tools for risk assessment, economic assessment, and risk management to counter terrorism. CREATE accomplishes this mission through an integrated program of research, education, and outreach, spanning the disciplines of economics, psychology, political science, industrial and systems engineering and information science. CREATE develops models, analytical tools, methodologies and software, and tests these tools in case analyses, representing critical homeland security investment and policy decisions.

Due to the cross-cutting nature of research in risk, economics, and risk management, CREATE serves the need of many client agencies at the DHS, including the Transportation Security Agency, Customs and Border Protection, Immigration and Customs Enforcement, FEMA and the US Coast Guard. In addition, CREATE has developed relationships with clients in the Offices of National Protection and Programs, Intelligence and Analysis, General Council, Health Affairs, and Domestic Nuclear Detection. Using a mix of fundamental and applied research, CREATE faculty and students take both the long-term view of how to reduce terrorism risk through fundamental research and the medium-term view of how to improve the cost-effectiveness of counter-terrorism policies and investments through applied research.

Please visit www.create.usc.edu for more information.
Innovations in Risk and Economic Modeling of Counterterrorism
Vicki Bier, University of Wisconsin-Madison
bier@engr.wisc.edu

1. Executive Summary ................................................................. 34
2. Research Accomplishments ....................................................... 42
  2.1. Probabilistic Inversion .......................................................... 42
  2.2. Target-Oriented Utility Theory for Counterterrorism ................. 64
3. Applied Relevance ................................................................. 94
  3.1. Probabilistic Inversion .......................................................... 94
  3.2. Target-Oriented Utility Theory for Counterterrorism ................. 105
4. Collaborative Projects ............................................................ 105
  4.1. Publications and Reports ...................................................... 116
  4.2. Presentations - Conferences .................................................. 127
  4.3. Presentations – Outreach ...................................................... 138
5. Education and Outreach Products ............................................. 138

1. Executive Summary

The development of game-theoretic models for homeland security has advanced quite rapidly, to the point where those models are almost ready for use in real-world decisions. The primary focus of the research at the University of Wisconsin-Madison has been to provide decision makers with practical yet rigorous ways to effectively and efficiently quantify and solve game-theoretic models of realistic size and complexity. In particular, this work addresses two of the most significant hurdles to making the economic tool of game theory applicable in homeland security in practice; namely, the need to quantify uncertain adversary preferences using subject-matter experts, and the need for sufficiently powerful computational tools to solve realistic defender problems within acceptable time constraints and levels of accuracy.

In previous years, we developed an elicitation process in which subject-matter experts are asked to give only ordinal judgments on the attractiveness of terrorist targets or strategies. Estimates of uncertain terrorist preferences (represented by a multi-attribute utility function) are then derived mathematically through the use of probabilistic inversion (PI). In the past year, our primary theoretical accomplishment was to adapt a related but different mathematical approach, Bayesian density estimation (BDE), to apply to ordinal judgments in a similarly rigorous manner. BDE complements PI; in particular, it extracts more information from the experts (especially regarding “schools of thought,” or subgroups of experts with positively correlated judgments). Hence, it is appropriate for use when there are sufficient experts for such correlations to be statistically meaningful, but may be less useful than PI when only small numbers of experts are available. We developed an efficient algorithm based on Gibbs sampling to estimate the BDE model, whose computation time grows only linearly with the size of the problem. Moreover, we explored the theoretical relationship between PI and BDE, elucidating under which conditions they give identical versus different results. Finally, we showed how PI and BDE differ in handling expert consensus or disagreement. These comparisons provide useful guidance on when and whether to use PI or BDE in real-world elicitation practice.

In additional analyses, we applied PI to ordinal judgments obtained from “proxy experts” (e.g., graduate students knowledgeable about terrorism, from parts of the world where support for terrorism is reasonably common, and found that the results compared reasonably well to those obtained by direct elicitation. We also found that both PI gave realistic results when applied to partial rankings of only a subset of targets, rather than full ranking of all targets; this is important for the application of PI in practice, since experts are unlikely to be willing or able to give detailed rankings of large numbers of targets.

Then, we developed two extensions to both PI and BDE, to enhance their applicability to real-world elicitation tasks. In particular, we extended both approaches to allow for negative attribute weights, to account for the possibility that experts may disagree about whether a larger value of a particular attribute yields higher or lower utility to the adversary (e.g., whether an adversary is seeking or is averse to high fatalities resulting from an attack). This is
important, especially when the number of experts is large (e.g., when using on-line surveys), because it makes it possible to analyze even results from experts with opposing views in an automated manner. We also extended both PI and BDE to handle ties in ordinal judgments, since in practice, experts may believe that multiple targets or attack strategies are equally attractive to the adversary (or may be unable to distinguish between their attractiveness), and hence give tied rank orderings for them.

Finally, we are also working on models of attacker deterrence. Achieving effective attack deterrence generally requires decreasing the success probability of an attack (or, conversely, increasing the cost of a successful attack) beyond the threshold considered tolerable by the prospective attacker. However, that threshold is not known. Therefore, we are using a new method known as target-oriented utility theory that makes it possible to minimize the probability of failing to achieve an uncertain target (e.g., in our case, the deterrence threshold). In the past year, we have applied this method to problems of network security, taking it beyond simple series or parallel systems to more realistic problems of interest in the real world.

Keywords: expert elicitation, uncertainty, ordinal judgments, adversary preferences, game theory, attacker deterrence

2. Research Accomplishments

2.1. Probabilistic Inversion

The development of game-theoretic models for homeland security has advanced quite rapidly, to the point where those models are almost ready for use in real-world decisions. The primary focus of the research on this task has been to provide decision makers with practical yet rigorous ways to effectively and efficiently quantify and solve game-theoretic models of realistic size and complexity. In particular, the goal of this work is to address two of the most significant hurdles to making the tool of game theory applicable to homeland security in practice—namely, the need to quantify uncertain adversary preferences using subject-matter experts, and the need for sufficiently powerful computational tools to solve realistic defender problems within acceptable time and accuracy.

In our model, we represent attacker preferences over targets or attack strategies using a multiple-attribute utility function, which can account for attacker preferences over both attack difficulty and the damage resulting from an attack, and also allows for unobserved attributes that may be important to the attacker but have not been identified or observed by the defender. We represent the defender’s uncertainty about the attacker’s preferences by probability distributions for the weights on the various attributes.

We developed a practical yet methodologically rigorous method of eliciting expert knowledge about the attribute weights in these multiple-attribute utility functions, using only ordinal judgments from intelligence analysts. The resulting approach simplifies the task of quantifying intelligence information for subject-matter experts by asking only for simple ordinal rankings on the attractiveness of particular targets or attack strategies, and may therefore increase the acceptance of quantitative approaches to risk estimation in the intelligence community. Two different mathematical methods, PI and BDE, have been used to infer cardinal estimates of attribute weights from the stated rank orderings, taking advantage of the fact that attribute weights must sum to one. The results provide information on the weights of the known attributes, and also information about how well the observed attributes explain the expert rankings (based on the weight assigned to an unobserved attribute).

During the past year, we have explored the relationship between PI and BDE, and developed efficient computational algorithms for BDE. Moreover, we also conducted sensitivity analysis to elucidate how PI and BDE handle consensus or disagreement existing among the intelligence experts, which would guide their usage in real-world adversary preference elicitation tasks.

We found that PI exploits only marginal rank orderings, whereas BDE captures correlations among judgments provided by the intelligence experts. Furthermore, BDE can place weight on the decision maker’s own judgment (rather than only the expert responses). If zero weight is placed on the decision maker’s judgment, then PI and BDE
are equivalent when there is only one expert, or when all experts give the same rank ordering of terrorist targets or strategies. In other cases, the PI result will coincide with the BDE result corresponding to the highest entropy among all possible ordinal judgments that satisfy the given marginal rank orderings. Moreover, our results suggest that BDE is more likely than PI to yield multimodal probability distributions for attribute weights in the face of expert disagreement. These features make PI suitable to use when expert judgments are not highly reliable (e.g., when using only a small number of experts to represent the views of a much larger population), in which case we may not want to put too much weight on the observed correlations among, and differences between, experts. However, BDE uses additional information not used by PI, on the correlations among experts, so it may be more appropriate when information from large numbers of experts is available, making it possible to distinguish reliably between different “schools of thought.”

As part of a related project on modeling of adaptive adversaries, we also applied PI to realistic ordinal data obtained from “proxy experts” (graduate students knowledgeable about terrorism, from parts of the world where support for terrorism is relatively common). That analysis provided favorable evidence regarding the usefulness and applicability of PI and related ranking-based methods in practice.

First, the following figure shows that results obtained using PI compare favorably to results obtained by direct elicitation using the random utility method of Richard John. As can be seen, both PI and direct elicitation identified the same three scenarios as being the least attractive (Pneumonic Plague, Dirty Bomb, and Blister Agent), and both methods assigned relatively high utilities to another three scenarios (Chlorine Tank Explosion, Improvised Explosive Device, and Food Contamination). The only significant discrepancies were in the utilities of Nerve Agent and Aerosol Anthrax (which were rated high using PI, but quite a bit lower using direct elicitation). However, we could take advantage of such discrepancies as input for convergent validation -- e.g., by asking proxy experts whether they put more credence in their scenario rankings or his directly assessed attribute weights.

Second, results indicated that preferences obtained based on a full ranking of all alternatives were quite similar to those obtained based on only a partial ranking; see comparison below. That figure compares the results of PI using the complete set of eight scenario rankings given by one proxy expert, versus only four rankings (the top three most attractive scenarios, and the least attractive scenario). The two sets of expected utilities are quite close, supporting the feasibility of applying PI to partial rankings in practice.

We also developed two extensions to both PI and BDE that are likely to be important in real-world applications. We first extended the methods to allow for negative attribute weights. Elicitation results with only non-negative attribute weights may incorrectly suggest that a given attribute is irrelevant to adversaries. For example, if an expert gives high rankings to some less populated targets, but the judgments are analyzed under the assumption that all attribute weights must be non-negative, that may incorrectly suggest that the adversary’s weight on fatalities is close to zero, when in fact the expert may believe that the adversary actually has an aversion to large numbers of fatalities (e.g., because attacks involving large numbers of fatalities could lead to reduced support for the terrorist’s cause, and/or massive U.S. retaliation). Allowing for negative weights can avoid this pitfall by making it possible for the results of the analysis to accurately reflect whatever opinions are inherent in the stated judgments.
Another extension to both PI and BDE was to allow for tied rank orderings when applying PI or BDE, for experts who either believe that several different targets are equally attractive to the attacker, or are totally uncertain about which of the tied targets is more attractive.

2.2. Target-Oriented Utility Theory for Counterterrorism

During the past year, we began efforts to apply our previous model of deterrence using target-oriented utility (Bordley and Kirkwood, 2004) to the problem of resource allocation for transportation-network security. In that regard, we considered two different transportation models.

In the first model, we considered the effects of congestion on the travel choices of individual drivers. Here, if one or more arcs on a transportation network are disrupted by an attack, then the remaining arcs will suffer greater congestion. If the shortest possible travel time from an origin to a destination is longer than the “reservation travel time” representing the value of the trip to a particular traveler, then that traveler will choose not to travel. Global optimization can be used to minimize the total of all travel times, plus the reservation times of those individuals who do not travel. Alternatively, individual travelers may be assumed to choose the fastest route between their origin and destination pairs in a decentralized manner. Global optimization is relatively straightforward; we are still working on modifying the model to allow for the decentralized “user equilibrium” problem, which is more realistic but substantially more challenging to solve.

The following graph shows a simple example transportation network with four nodes. Travelers can go from node 1 to node 4 (on either the red arcs, through node 2, or the blue arcs, through node 3); there are also travelers from node 4 to node 1 (on either the purple arcs, through node 2, or the green arcs, through node 3). There are a total of 172 travelers wanting to go from node 1 to node 4, and 843 travelers wanting to go from node 4 to node 1. Reservation travel times for both sets of travelers are uniformly distributed between 13.683 and 25.656. In other words, everyone will want to travel if the travel time is less than 13.683, but nobody will want to travel if the travel time is more than 25.656; for intermediate travel times, a fraction of travelers will choose to travel, depending on whether the travel time is above or below their reservation travel times. Results that are computed using the model (rather than assumed as input to the model) are shown in bold font in the tables below.
Results show that 98.7% of those wishing to go from node 1 to node 4 are able to travel, but only 95.6% of the much larger number of individuals wishing to go from node 4 to node 1. Of those going from node 1 to node 4, 34 travelers go through node 2, and 136 go through node 3. Conversely, of those travelers going from node 4 to node 1, 357 go through node 2, and 449 through node 3. In general, travelers going through node 2 have a slightly higher speed than those going through node 3, but that is counteracted by the fact that the arcs going through node 3 are slightly shorter, resulting in roughly equal travel times through either node. Next steps in this model development are to show the effects of attacks on congestion and route choices (i.e., if some arcs have been disabled), and to model the optimal defensive investment in each arc. Here, target-oriented utility will be used to reflect the fact that the defender does not know the cost of attacks to the attacker, and hence the level of defensive investment at which the attacker will be deterred.

In the second model, we considered the optimal placement of sensors (e.g., radiation detectors) on a transportation network. Here, the usual approach is to maximize the probability of attack detection; however, this may result in wasted resources, if something less than the maximum achievable detection probability may still deter an attack. Hence, we take advantage of target-oriented utility theory to reformulate the defender’s model as one of maximizing the probability of successfully deterring an attack, where the magnitude of the detection probability needed to deter an attack is assumed to be uncertain. In order to capture this uncertainty, we assume that the defender’s uncertainty about the threshold detection probability at which the attacker would be deterred follows a Kumaraswamy distribution (Jones 2009). This distribution is convenient,
since it is defined over a domain of \([0, 1]\), like the beta distribution, but has the advantage of a simple closed-form cumulative distribution function.

In this model, we have a directed graph of nodes and arcs representing the transportation network, one attacker who attempts to traverse the network, and one defender who seeks to deter the attacker through placement of sensors. (Travelers other than the attacker may also traverse the network, of course, but they are not relevant to this model.) The attacker starts from an origin node and attempts to reach a specific destination node (e.g., to deliver a dirty bomb or nuclear weapon to some preferred target in the network). The attacker chooses which arcs to traverse in order to reach his destination with the minimum probability of being detected, but will be deterred from attacking at all if the chance of detection is above some threshold (where the defender is uncertain about the value of this threshold). If the attacker successfully reaches the target node, a loss \(L\) will be incurred by the defender. The defender allocates her resources to invest in defense of selected arcs, where placement of a sensor on arc \(ij\) is assumed to reduce the probability of the attacker successfully traversing that arc from \(p_{ij}\) to \(q_{ij} < p_{ij}\). The defender decides which arcs to protect in order to minimize expected loss plus total investment, where the expected loss is given by the loss \(L\), times the probability of the attacker successfully traversing the network if an attack is attempted, times the probability that the attacker attempts an attack.

See the figure below to see how the defender’s optimum investment level depends on the loss \(L\). As the damage to the defender from a successful attack grows, the defender is willing to invest in protection of additional arcs. This is reflected in the step increases in the total level of defensive investment at optimality.
3. Applied Relevance

3.1. Probabilistic Inversion

In order for game theory to be a readily usable tool for homeland-security decision making, it is essential to be able to quantify the decision maker’s uncertainty about attacker preferences. However, eliciting information on adversary utility functions from individuals knowledgeable about terrorism is difficult, since many intelligence experts are not quantitatively trained, and may not be familiar with multiple-attribute utility theory. Moreover, many intelligence experts place a great deal of importance on achieving consensus, which is not conducive to accurately characterizing the level of uncertainty that may exist. As a result, there is a need for indirect elicitation methodologies to “translate” information of the type that intelligence experts feel comfortable providing into risk-assessment “language.”

We believe that the indirect elicitation method we have developed can lead to greater acceptance of quantitative approaches in the intelligence community, by allowing experts to provide their judgments in the form most meaningful to them. In addition, it can sometimes also lead to improved accuracy. For example, experts who are asked to provide attribute weights directly may place inappropriately high weight population density, without realizing that Jersey City actually has a much higher population density than more attractive terrorist targets such as New York, Los Angeles, or San Francisco. Experts who are given the opportunity to rank the attractiveness of targets directly would be unlikely to make put high weight on population density, since they presumably would not weight Jersey City as a top terrorist target, so attribute weights inferred from expert judgments of target attractiveness might result in more realistic weights.

The methods developed in this work have already been applied to realistic estimates of terrorist preferences over attack scenarios in a separate project on modeling of adaptive adversaries funded by the Department of Homeland Security. The fact that the model has now been extended to allow for negative attribute weights and ties in expert rankings means that it is now usable for eliciting the opinions of large number of experts in an automated (e.g., online) manner. Potential customers include the Office of Strategy, Planning, and Analysis at DHS; staff members there have expressed interest in software development for expert elicitation of terrorist preferences, not as a simpler alternative to traditional elicitation, but as a means of convergent validation to achieve greater reliability and credibility than traditional expert-elicitation methods alone. We also reached out to potential users of our elicitation methods at Argonne National Laboratory. In particular, they have provided us data on rankings of adversary threats.

Optimum total investment as a function of $L$
against particular sectors (e.g., transportation systems, government facilities, etc.) using particular attack strategies (e.g., active shooters, improvised explosive devices, etc.), for use in validating our models.

3.2. Target-Oriented Utility Theory for Counterterrorism

Investments in homeland security are intended only partly to reduce vulnerability and consequences in the event of an attack; they are also intended in part to reduce the threat, by deterring possible attacks. Achieving effective attack deterrence generally requires decreasing the success probability of an attack (or, conversely, increasing the cost of a successful attack) beyond the threshold considered tolerable by the prospective attacker. Since that threshold is not known, modelers often strive to minimize the success probability of an attack (or, less commonly, maximize the cost of launching a successful attack). However, this approach can result in wasted resources, if the level of security achieved through the optimization process is greater than that needed to deter attacks. The application of target-oriented utility theory to deterrence modeling can address this challenge.

Although our models of deterrence using target-oriented utility theory are not yet ready for direct application, the fact that we are successfully developing and applying such models to transportation networks demonstrates that they are scalable to real-world problems. In particular, ongoing work is applying target-oriented utility theory both to problems of sensor placement on a transportation network (with the goal of using sensors to deter terrorists from attempting to deliver weapons of mass destruction through the network), and to problems of network disruption and congestion (with the goal of using defensive investment in protection of the network to discourage terrorists from attempting to disrupt transportation networks).

4. Collaborative Projects

The project on probabilistic inversion benefited greatly from close interactions with the CREATE team working on adaptive-adversary modeling under separate funding from the Department of Homeland Security. That project made it possible for us to test our methods on realistic input data, and also compare both the resources required for our method and the results with those of direct elicitation.

In addition, the principal investigator on this project, Vicki Bier, also worked on a grant from the Wisconsin Office of Justice Assistance to characterize both safety and security risks to pipelines in the state of Wisconsin. The Office of Justice Assistance is the organization that distributes funds from the Department of Homeland Security (e.g., the Buffer Zone Protection Program and other similar security programs) in Wisconsin. In addition to the Office of Justice Assistance, the project also involved input from, and interactions with, the Protective Security Adviser for the state of Wisconsin, as well as the Wisconsin Department of Natural Resources, the Wisconsin Public Service Commission, and Wisconsin Emergency Management.

Finally, in collaboration with Jun Zhuang at Buffalo, a project was recently funded by the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland. The purpose of that project is to conduct a workshop on how to actually validate models of adversary behavior, with the goal of producing a special issue of a journal on that topic. We are currently approaching possible journals that might house such a special issue, and developing lists of workshop attendees (to include both developers of theoretical models and also experts on the use of empirical data), and are hoping to hold the planned workshop next June.
4.1. Publications and Reports

### CREATE PUBLICATIONS

**Bier, Vicki - University of Wisconsin - Madison**


4.2. Presentations - Conferences


4.3 Presentations – Outreach

1. Sinan Tas, Resilience and vulnerability of complex systems: A case study on electric power networks, Penn State Berks, Department of Information Sciences and Technology, spring 2012


5. Education

<table>
<thead>
<tr>
<th>CREATE STUDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Name</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>1. Ertem</td>
</tr>
<tr>
<td>3. Hu</td>
</tr>
<tr>
<td>7. Okpara</td>
</tr>
<tr>
<td>8. Tas</td>
</tr>
<tr>
<td>10. Welburn</td>
</tr>
<tr>
<td>11. Hoerning</td>
</tr>
</tbody>
</table>
Research topics not directly supported by CREATE:

Mehmet Ertem is working on a defender-attacker model for security of computer networks, using attack graphs to represent the possible attacker strategies and defender options. In the literature, most network-interdiction models allow the attacker only one attempt (assuming that the attacker is captured and disabled after a single failure); other models allow multiple attempts, but assume that any subsequent attempt begins at the point in the network where the previous attempt failed. These models are not appropriate for computer security, where the attacker could be operating from the safety of a foreign country, and the cost of starting over with a completely different attack strategy may be quite low. To represent the ability of the attacker to launch multiple attempts, we represent the attacker’s success or failure on any one arc of the attack graph probabilistically, and formulate the resulting security problem as a multiple-stage stochastic network-interdiction problem. In the resulting game, a non-myopic defender anticipates both the attacker’s strategy choices and their probabilities of success or failure, and chooses a single defensive strategy (i.e., a set of arcs in the attack graph to protect) by which to defend against multiple attempted attacks. The attacker then launches an optimal attack against the system, assuming knowledge of which arcs have been protected. We solve the resulting stochastic-optimization problem using two-stage stochastic optimization with recourse, and explore the attacker’s attack strategies and the defender’s optimal defense strategy.

Greg Hammond is currently working on a project that seeks to improve protective-action strategies following a nuclear-power emergency. Current evacuation protocols are based on pre-established emergency protective zones. In this study, a heuristic is being developed to dynamically create "right-sized" protective-action zones from plume forecasts using event-specific and situation-specific data. As part of the study, the heuristic will also be compared to evacuation strategies that are currently approved by the Nuclear Regulatory Commission. The goal is to achieve comparable radiological protection with smaller and more targeted evacuation zones. His graduate education is supported by the U.S. Air Force, for which he is currently an active-duty officer.

Wen-Chieh Hu is working on extending past work on interdependent security with heterogeneous discount rates. The goal of the extension is to allow defenders to make continuous investments in defense (fractional defenses), rather than just a binary choice of defending or not.

Taher Jamshidi collaborated with Vicki Bier and Mavis (Chen) Wang on the adaptive-adversary project funded by the Department of Homeland Security. In addition, he is working on investment in preparedness by private firms. In particular, his game-theoretic model of investment suggests that the dynamics of market competition can create a "race to the bottom," since firms that invest in preparedness may find themselves saddled with excess costs if several years pass without the occurrence of a disaster. In order to model this characteristic behavior of the market, our model incorporates negative externalities. Preliminary results suggest that the equilibrium solution to this game will often involve preparedness investment by some but not all firms in the market, where some firms "bet" on the occurrence of a disaster and others bet that a disaster will not occur; perhaps surprisingly, it does not always matter which firm(s) invest at equilibrium and which do not, even when the firms are heterogeneous. We plan to characterize how the equilibrium outcomes to this game depend on parameters such as the cost of preparedness, the fixed and variable costs of productions, and the frequency of disasters. We will also explore circumstances in which measures may be needed to help reach the social optimum level of preparedness if that differs from the equilibrium solution to the game.
Uche Okpara recently completed his Ph.D. from the University of Wisconsin-Madison. His dissertation involved a game-theoretic study of the threat to commercial aviation from man-portable air defense systems. His model addressed how potential attackers might respond to particular types of countermeasures (e.g., by shifting to less capable or less reliable weapons systems that are less susceptible to the implemented countermeasures), and also took into account the geometry of the problem (e.g., attacker distance from targeted aircraft, attacker targeting strategies, etc.).

Sinan Tas also recently completed his Ph.D. from the University of Wisconsin-Madison. His dissertation involved a game-theoretic vulnerability-assessment model for electric-power systems that is capable of taking into account cascading failures and restoration time, as well as the initial unmet demand that could be anticipated to arise from intelligent attacks. He has taken a position as an assistant professor in the Department of Information Sciences and Technology at Penn State Berks, where he is teaching courses on risk analysis, computer security, and homeland security. He hopes to extend his dissertation research to apply to telecommunications security and computer security as well as electric-power security.

Jon Welburn and Steve Hoerning are currently working on a model of food-import safety. In particular, they are using violations data from the Operational and Administrative System for Import Support (OASIS) maintained by the U.S. Food and Drug Administration to assess the risk of food imports by product type and country of origin. The goals are to address rising concerns about food safety, quantify the risks, and explore the usefulness of OASIS data for practical risk management.

In addition, Jon Welburn is working on a model of global economic risk. The goal is to compare the assumed propagation of adverse economic risks from one country to another (using the “contagion” model typical in macroeconomics) with the common-cause model common in engineering (where multiple failures are assumed to be correlated with each other, but not directly causative of subsequent failures). He is supported for this work by an NSF fellowship. As part of this project, he received NSF funding to study with Kjell Hausken, Professor of Economics at the University of Stavanger in Norway (and a CREATE affiliate), in summer 2012.

CREATE RELATED COURSES

<table>
<thead>
<tr>
<th>Instructor</th>
<th>University</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Bier</td>
<td>UW Madison</td>
</tr>
<tr>
<td>2.</td>
<td>Bier</td>
<td>UW Madison</td>
</tr>
<tr>
<td>3.</td>
<td>Bier</td>
<td>UW Madison</td>
</tr>
</tbody>
</table>

<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>4</td>
</tr>
<tr>
<td># of students involved (funded by CREATE + any other programs)</td>
<td>11</td>
</tr>
<tr>
<td># of students graduated</td>
<td>2</td>
</tr>
<tr>
<td># of contacts with DHS, other Federal agencies, or State/Local (committees)</td>
<td>29 (see below)</td>
</tr>
<tr>
<td># of existing courses modified with new material</td>
<td></td>
</tr>
<tr>
<td># of new courses developed</td>
<td></td>
</tr>
<tr>
<td># of new certificate programs developed</td>
<td></td>
</tr>
<tr>
<td># of new degree programs developed</td>
<td></td>
</tr>
</tbody>
</table>

Argonne National Laboratory (James Peerenboom, David Brannegan, Patrick Wilkey, Julia Phillips, Jeffrey Western, Ron Whitfield, Bill Buehring, Lon Carlson, Gib Bassett)

Dane County Emergency Management (J. McLellan)
6. Outreach

Student Greg Hammond was the co-chair for the Glacier Edge Elementary School 2012 Science Fair in Verona, WI.


Vicki Bier offered a “University Summer Forum” in summer 2012 on the subject Masters of Disaster: Lessons Learned from Catastrophic Events. Summer Forums open to the public at no cost and to registered students for the regular credit fees.