Project Title: Optimal Partnership Strategies for Cyber Threats

This project will integrate operations research and game theory to study the optimal partnership strategies among governmental agencies and private sectors, to prepare for and recover from cyber attacks. This project will develop novel models, and transit the results to homeland security practitioners.

1. Theme Area: Risk Analysis – Management of Risks from Intelligent, Adaptive Adversaries
2. Principal Investigator: Jun Zhuang
3. Institution: University at Buffalo
4. Co-Investigators: None
5. Research Transition Lead: Jun Zhuang
6. Keywords: Game theory, cyber security, partnership, information sharing, intelligence,

7. Brief Description: The purpose of this research is to integrate operations research and game theory to study the optimal partnership strategies among governmental agencies and private sectors, to prepare for and recover from cyber threats. This project was originally motivated by PI’s conversation with DHS decision makers and FBI agencies, where the partnership and information/intelligence sharing between and among governmental/private sectors were identified to be critical for enhancing cyber security. Such information sharing activities are generally voluntary, and each agency independently makes decisions about partnership. One recent National Institute of Standards and Technology (NIST) report (Johnson et al., 2014) says “To enhance incident response actions and bolster cyber defenses, organizations must harness the collective wisdom of peer organizations through information sharing and coordinated incident response.”

This project will provide insights on governmental and private sectors’ partnership strategies in a cyber security context, by helping addressing questions: (a) whom should agencies share information and partner with? (b) what are the optimal levels of information/resource sharing? (c) what are the tradeoffs and optimal balance between public and private investment in cyber security? (d) what types of incentives/subsidies should be provided to whom in order to achieve the socially optimum level of partnership? and (e) what is the optimal balance between pre-event prevention/preparedness and post-event relief/investigation in cyber security? It is important in the homeland security practice to fill these gaps. In particular, practitioners do not have clear guidelines on how to optimally balance the above tradeoffs and maximize cyber-awareness through partnership. If successful, this research will help to generate practical insights and guidelines, and thereby, improve cyber security practices.

8. Research Objectives: The objectives of this project are: (a) explore new modeling frameworks to evaluate the incentives implicit in governmental and private sectors’ partnership strategies in cyber security; (b) study the tradeoffs in incentive provisions between prevention and investigation, and between private and public investment in countermeasures; (c) transit the results to homeland security practitioners; and (d) provide education and outreach to high
school/undergraduate/graduate students, and governmental/private sectors who would be concerned about cyber security.

9. Research Transition Objectives: This project will develop models and tools to be used by DHS personnel in carrying out their analysis prior to making decisions. For example, the responsibility of the Office of Cybersecurity and Communications (CS&C) is for “enhancing the security, resilience, and reliability of the Nation’s cyber and communications infrastructure.” We will develop optimal partnership models and tools with close collaboration with end users at CS&C and Office of Strategy, Planning, Analysis and Risk at DHS.

10. Interfaces to Current CREATE Projects: This work will maintain a close interface with many CREATE projects on risk, economic, and game-theoretic modeling of adversaries. In particular, this project could complement to the following current CREATE projects: (a) “Deterring Adaptive Adversaries: Multi-Attribute Utility (MAU) Analysis, Decision Trees and Value of Misinformation for Informing Cyber Security” led by Drs. Richard John and Heather Rosoff; (b) “Towards an Economic Behavioral Science Approach to Cyber Security” led by Dr. Scott Farrow; (c) “Development of Big Data Analytics for Infrastructure System Security” led by Drs. Michael Orosz, Daniel Salazar, Samrat Chatterjee; (d) “Economic Consequences of Terrorism” led by Dr. Adam Rose; and (e) “Validating Models of Adversary Behavior” led by Dr. Jun Zhuang. Specifically, many data from to those projects could be used to quantify, calibrate, and exercise the models to be developed in this project.

11. Previous or Current Work Relevant to the Proposed Project: The PI has have been continuously supported by CREATE since Spring 2004 on modeling adaptive adversaries. Additionally, the PI has been working with the researchers at Oak Ridge National Lab, Air Force Research Lab, and US Army Engineer Research and Development Center on game-theoretical models in security and defense. This project in particular leverage the PI’s DOE project “Game Theoretic Modeling of Attacks and Defenses in Cyber-Physical Networks.” The PI is working on a 3-year NSF grant “Robust Approval Process in the Face of Strategic Adversaries and Normal Applicants,” which uses game-theoretical and queuing models to study the interactions between the government and (normal and adversarial) applicants. The PI is also working on a 3-year NSF grant “Incentives in Government Provision of Emergency Preparedness and Disaster Relief,” which uses game theory to study optimal partnerships between public and private sectors facing natural disasters. This CREATE project will extend the above theoretical models to cyber security context as well as outreach to DHS agencies.

12. Major Deliverables, Research Transition Products and Customers: This project will produce: (a) software demos for homeland security practitioners and private sectors, illustrating the dynamics of optimal partnership and resource sharing strategies as input parameters change; (b) practical insights and guidelines documented in reports and handbooks for homeland security practitioners and communities; (c) peer-reviewed journal articles and conference presentations; and (d) news reports and media coverage.

Potential customers include: (a) Office of Cyber Security and Communications and Office of Strategy, Planning, Analysis and Risk at DHS; (b) other DHS agencies such as U.S. Computer Emergency Readiness Team, Transportation Security Administration (TSA), and Customs and
Border Protection (CBP); (c) other federal agencies, including U.S. Cyber Command, Office of the Director of National Intelligence, FBI/InfraGard, researchers at Oak Ridge National Laboratory and U.S. Army Engineer Research and Development Center; and (e) other private sectors, government agencies and non-government organizations.

13. Technical Approach: The methods developed will build on the PI’s previous research on game theory and operations research methods for optimal homeland security resource allocation. Figure 1 introduces the basic research framework of this proposed project. This project intends to model a variety of games among the players including governments and private sectors for cyber security context as well as other disasters. The players seek to protect business/trade secrets, intellectual properties, critical infrastructure and lives, from both adaptive threats (e.g., cyber threats, terrorism, which will be modeled as a player in the game) and non-adaptive threats (e.g., natural disasters and technological hazards). In particular, the players are connected in a network and may detect threats by themselves and then decide how (and what, to whom) to share such information/intelligence (e.g., reporting suspicious behavior to www.ic3.gov), either on a regular, or an intermittent basis. Federal government can provide grants to local governments and aid to foreign governments; and all levels of government can provide pre-event preparation and post-event relief/investigation to private sectors. The government can also outreach and provide incentives and subsidies to promote awareness of cyber threats among private sectors. Private sectors can also, of course, make their own decision on partnership, information sharing, and investments in countermeasures (e.g., purchasing security service, minimizing exposure of critical information, or training employees). To study progressively more complex and realistic scenarios, this project will explore models with incomplete information, multi-player (Zhuang 2010), multi-period (Hausken and Zhuang 2011), and risk-seeking or risk-averse preferences (Zhuang and Bier 2007). This project will also explore the use of various multi-attribute utility functions to model the players’ objectives and payoffs (Keeney and Raiffa 1976), including preferences for the multi-dimensionality of cyber attack consequences (Keeney 2007). We also plan to closely with our partners to validate and verify the models, and provide them the software demos and computerized decision support tools.

Task A. Private-Private Partnership on Information and Resources Sharing:
Figure 2: Partnership networks (a) and (b) were developed from interviews conducted in Haiti during the summer of 2010, supported by the PI’s NSF RAPID award. In this project, we plan to interview private and public agencies on their information sharing patterns and strategies, in the face of cyber threats and other disasters.

First, pending IRB approval, we plan to interview private sectors on their practices and concerns of information and resource sharing, and construct partnership networks. Figure 2 shows some similar partnership network for the NGOs before and after Haiti earthquake, using the interview data from the PI’s NSF RAPID project. We plan to use random sampling (agency recruitment as they are identified during yellowpage, online, or through other means) and snowball sampling (agency recruitment using the connections of agencies already participating in the study) to maintain and increase the pool of participants. We acknowledge the potential sampling bias and will leverage multiple logistic regression, mean difference of variables, restriction/enhancement of variances (Goodman and Blum, 1996) to minimize the impact of such biases (Beauchemin and Gonzalez-Ferrer, 2011). Second, we plan to use mathematical modeling to depict the partnership strategies as a resource sharing game, and compare the equilibrium strategies with our empirical results. In particular, each of the players will independently decide who to share resources/information using their own (expected) costs and benefits of doing so, which form an equilibrium. (Government incentives/regulations will be treated as exogenous parameters in Task A, but will be modeled endogenously in Task B.)

Task B. Public-Private Partnership for Cyber Threats:
Public and private investment for preparing for and mitigating cyber threats can be either substitutes or complements, depending on the particular context.

Figure 3: Costs and Expected Losses as Functions of the Level of Subsidies, where V is target valuation.

To illustrate, we consider a sequential game between two players. The government decides the amount of subsidy s to provide to a private sector, and the private sector decides on the amount of private investment p. We assume that the subsidy s and the private investment p jointly reduce the probability of damage. The total societal cost U equals the sum of the subsidy s, the private investment p, and the expected damage P(s,p)V, where V is the target valuation. We consider three levels of V: low (V = 0.5); medium (V = 2.5); and high (V = 5). Figures 3(a-b) show that when V is small or moderate, even when the provision of subsidy can induce private investment (when s>2 and s>0.4, respectively), the social optimum is still to provide zero subsidy. By contrast, when V is large, Figure 3(c) shows that the provision of 1.4 units of subsidy (which induces 1.4 units of private investment) leads to the minimal societal cost. We plan to model
these joint effects in the context of threat/disaster preparedness by borrowing the concept of an elasticity of substitution from economics, which provides a tunable parameter representing different types of joint effects (ranging from perfect substitutes to perfect complements). We plan to study equilibrium behavior in such models (including the levels of public and private investment, and the probability and consequences of disasters as a result of those investment levels) as a function of the elasticity. We also plan to work with practitioners to identify real-world examples where public and private investment are substitutes or complements, and use expert opinions and experiments to study the strength of such relationships. Government bills, subsidy, grants, rules, could serve as incentive or disincentive for private sectors to invest or share information within the cyber security context.

14. Major Milestones and Dates

- Conduct pre-brief with Cybersecurity Division to potentially re-define project scope – August 2015.
- Start constructing a user-friendly visualization and decision-support tools for optimal partnership in cyber security – September 2015.
- Demonstrate the results of the models and software during conferences, and monthly FBI/InfraGard-Buffalo meetings – From August 2015 to June 2016.
- Submit a journal article on balancing pre-event prevention and post-event investigation for cyber security – November 2015.
- Submit a journal article on optimal public-private partnership in cyber security – April 2016.
- Finalize the visualization and software demo and make it available online – April 2016.
- Secure additional applied projects from homeland security agencies based on this research – June 2016.

15. References:

16. CV:

Dr. Jun Zhuang is an Associate Professor of Industrial and Systems Engineering at the University at Buffalo, the State University of New York (UB, or SUNY-Buffalo). Dr. Zhuang has a Ph.D. in Industrial Engineering in 2008 from the University of Wisconsin-Madison. Dr. Zhuang's research has been supported by the NSF, the DHS through CREATE and START, by the Department of Energy through the Oak Ridge National Laboratory, and by the U.S. Air Force Office of Scientific Research (AFOSR) through the Air Force Research Laboratory. Dr. Zhuang is a recipient of the 2014 MOR Journal Award for the best paper published in 2013 in the journal *Military Operations Research*. Dr. Zhuang is a recipient of the UB's Exceptional Scholar—Young Investigator Award for 2013. Dr. Zhuang is also a fellow of the 2011 U.S. Air Force Summer Faculty Fellowship Program (AF SFFP), sponsored by the AFOSR, and a fellow of the 2009-2010 Next Generation of Hazards and Disasters Researchers Program, sponsored by the NSF. Dr. Zhuang has published 36 peer-reviewed journal articles and about 10 peer-reviewed conference proceedings/book chapters, gave 100+ conference presentations and 30+ research seminars in universities and research institutes in the U.S. and around the world.

Since August 2008, Dr. Zhuang has mentored about 20 undergraduate and graduate students on CREATE-sponsored projects. His students have won various student awards from Society for Risk Analysis, Decision Analysis Society, UB's Center for Undergraduate Research and Creative Activities, and UB’s Undergraduate Research and Scholarship Award of Distinction. Recently Dr. Zhuang won the prestigious 2012 Faculty Award for Excellence in Mentoring Undergraduate Research and Creative Activity from the UB. Dr. Zhuang’s CREATE-sponsored research in homeland security has received extensive national publicity. The PI was invited to be a panelist in the 2011 DHS Science Conference--Fifth Annual DHS University Network Summit in April 2011. Two of his Ph.D. students were also invited to present posters at the same conference. Dr. Zhuang’s research is listed under “Research News” on the website of the Stanford Graduate School of Business [www.gsb.stanford.edu/news/research/JunZhuang.html](http://www.gsb.stanford.edu/news/research/JunZhuang.html), following his invited presentation at *Operations Research for the Public Interest Conference* in June 2010. Dr. Zhuang was also featured as one of the “New Faces of Engineering 2009” (nominated by the Institute of Industrial Engineers and selected by National Engineers Week Foundation, [www.eweek.org/site/Engineers/newfaces2009/IIE.shtml](http://www.eweek.org/site/Engineers/newfaces2009/IIE.shtml), as “Extreme Engineer of the Month” (in *Pre-Engineering Times: A publication of the Junior Engineering Technical Society* for January 2008, and in *Industrial Engineer* magazine in March 2007, September 2010, and March 2012.