University Transportation Research Center - Region 2

Final Report

The Game-Theoretic National Interstate Economic Model: An Integrated Framework to Quantify the Economic Impacts of Cyber-terrorist Behavior

Performing Organization: University at Buffalo (SUNY)

December 2014

Sponsor:
University Transportation Research Center - Region 2

University Transportation Research Center - Region 2

The Region 2 University Transportation Research Center (UTRC) is one of ten original University Transportation Centers established in 1987 by the U.S. Congress. These Centers were established with the recognition that transportation plays a key role in the nation's economy and the quality of life of its citizens. University faculty members provide a critical link in resolving our national and regional transportation problems while training the professionals who address our transportation systems and their customers on a daily basis.

The UTRC was established in order to support research, education and the transfer of technology in the field of transportation. The theme of the Center is "Planning and Managing Regional Transportation Systems in a Changing World." Presently, under the direction of Dr. Camille Kamga, the UTRC represents USDOT Region II, including New York, New Jersey, Puerto Rico and the U.S. Virgin Islands. Functioning as a consortium of twelve major Universities throughout the region, UTRC is located at the CUNY Institute for Transportation Systems at The City College of New York, the lead institution of the consortium. The Center, through its consortium, an Agency-Industry Council and its Director and Staff, supports research, education, and technology transfer under its theme. UTRC's three main goals are:

Research

The research program objectives are (1) to develop a theme based transportation research program that is responsive to the needs of regional transportation organizations and stakeholders, and (2) to conduct that program in cooperation with the partners. The program includes both studies that are identified with research partners of projects targeted to the theme, and targeted, short-term projects. The program develops competitive proposals, which are evaluated to insure the mostresponsive UTRC team conducts the work. The research program is responsive to the UTRC theme: "Planning and Managing Regional Transportation Systems in a Changing World." The complex transportation system of transit and infrastructure, and the rapidly changing environment impacts the nation's largest city and metropolitan area. The New York/New Jersey Metropolitan has over 19 million people, 600,000 businesses and 9 million workers. The Region's intermodal and multimodal systems must serve all customers and stakeholders within the region and globally.Under the current grant, the new research projects and the ongoing research projects concentrate the program efforts on the categories of Transportation Systems Performance and Information Infrastructure to provide needed services to the New Jersey Department of Transportation, New York City Department of Transportation, New York Metropolitan Transportation Council , New York State Department of Transportation, and the New York State Energy and Research Development Authorityand others, all while enhancing the center's theme.

Education and Workforce Development

The modern professional must combine the technical skills of engineering and planning with knowledge of economics, environmental science, management, finance, and law as well as negotiation skills, psychology and sociology. And, she/he must be computer literate, wired to the web, and knowledgeable about advances in information technology. UTRC's education and training efforts provide a multidisciplinary program of course work and experiential learning to train students and provide advanced training or retraining of practitioners to plan and manage regional transportation systems. UTRC must meet the need to educate the undergraduate and graduate student with a foundation of transportation fundamentals that allows for solving complex problems in a world much more dynamic than even a decade ago. Simultaneously, the demand for continuing education is growing – either because of professional license requirements or because the workplace demands it – and provides the opportunity to combine State of Practice education with tailored ways of delivering content.

Technology Transfer

UTRC's Technology Transfer Program goes beyond what might be considered "traditional" technology transfer activities. Its main objectives are (1) to increase the awareness and level of information concerning transportation issues facing Region 2; (2) to improve the knowledge base and approach to problem solving of the region's transportation workforce, from those operating the systems to those at the most senior level of managing the system; and by doing so, to improve the overall professional capability of the transportation workforce; (3) to stimulate discussion and debate concerning the integration of new technologies into our culture, our work and our transportation systems; (4) to provide the more traditional but extremely important job of disseminating research and project reports, studies, analysis and use of tools to the education, research and practicing community both nationally and internationally; and (5) to provide unbiased information and testimony to decision-makers concerning regional transportation issues consistent with the UTRC theme.

Project No(s):
UTRC/RF Grant No: 49997-38-24 , DRTC-G-UTC02

Project Date: December 2014

Project Title: The Game-Theoretic National Interstate Economic Model: An Integrated Framework to Quantify the Economic Impacts of Cyber-terrorist Behavior

Project's Website:
http://www.utrc2.org/research/projects/national-aviation-security-cyber-terrorism-sharing-programs

Principal Investigator(s):

Dr. Jiyoung Park
University at Buffalo (SUNY)
05L Hayes Annex C
3435 Main St.
Buffalo, NY 14214
Tel: (716) 829-5331
Email: jp292@buffalo.edu

Co author(s):
Ha Hwang
Unversity at Buffalo (SUNY)

DongIn Cho
Sungkyunkwan University

Performing Organization:
University at Buffalo (SUNY)

Sponsor(s):
University Transportation Research Center (UTRC)

To request a hard copy of our final reports, please send us an email at utrc@utrc2.org

Mailing Address:

University Transportation Reserch Center
The City College of New York
Marshak Hall, Suite 910
160 Convent Avenue
New York, NY 10031
Tel: 212-650-8051
Fax: 212-650-8374
Web: www.utrc2.org

Board of Directors

The UTRC Board of Directors consists of one or two members from each Consortium school (each school receives two votes regardless of the number of representatives on the board). The Center Director is an ex-officio member of the Board and The Center management team serves as staff to the Board.

City University of New York
Dr. Hongmian Gong - Geography/Hunter College
Dr. Neville A. Parker - Civil Engineering/CCNY

Clarkson University
Dr. Kerop D. Janoyan - Civil Engineering

Columbia University
Dr. Raimondo Betti - Civil Engineering
Dr. Elliott Sclar - Urban and Regional Planning

Cornell University
Dr. Huaizhu (Oliver) Gao - Civil Engineering

Hofstra University
Dr. Jean-Paul Rodrigue - Global Studies and Geography

Manhattan College
Dr. Anirban De - Civil & Environmental Engineering
Dr. Matthew Volovski - Civil & Environmental Engineering

New Jersey Institute of Technology
Dr. Steven I-Jy Chien - Civil Engineering
Dr. Joyoung Lee - Civil & Environmental Engineering

New York University
Dr. Mitchell L. Moss - Urban Policy and Planning
Dr. Rae Zimmerman - Planning and Public Administration

Polytechnic Institute of NYU
Dr. Kaan OzbaÙ - Civil Engineering
Dr. John C. Falcocchio - Civil Engineering
Dr. Elena Prassas - Civil Engineering

Rensselaer Polytechnic Institute
Dr. José Holguín-Veras - Civil Engineering
Dr. William "Al" Wallace - Systems Engineering

Rochester Institute of Technology
Dr. James Winebrake - Science, Technology and Society/Public Policy
Dr. J. Scott Hawker - Software Engineering

Rowan University
Dr. Yusuf Mehta - Civil Engineering
Dr. Beena Sukumaran - Civil Engineering

State University of New York
Michael M. Fancher - Nanoscience
Dr. Catherine T. Lawson - City & Regional Planning
Dr. Adel W. Sadek - Transportation Systems Engineering
Dr. Shmuel Yahalom - Economics

Stevens Institute of Technology
Dr. Sophia Hassiotis - Civil Engineering
Dr. Thomas H. Wakeman III - Civil Engineering

Syracuse University
Dr. Riyad S. Aboutaha - Civil Engineering
Dr. O. Sam Salem - Construction Engineering and Management

The College of New Jersey
Dr. Thomas M. Brennan Jr - Civil Engineering

University of Puerto Rico - Mayagüez
Dr. Ismael Pagán-Trinidad - Civil Engineering
Dr. Didier M. Valdés-Díaz - Civil Engineering

UTRC Consortium Universities

The following universities/colleges are members of the UTRC consortium.

City University of New York (CUNY)
Clarkson University (Clarkson)
Columbia University (Columbia)
Cornell University (Cornell)
Hofstra University (Hofstra)
Manhattan College (MC)
New Jersey Institute of Technology (NJIT)
New York Institute of Technology (NYIT)
New York University (NYU)
Rensselaer Polytechnic Institute (RPI)
Rochester Institute of Technology (RIT)
Rowan University (Rowan)
State University of New York (SUNY)
Stevens Institute of Technology (Stevens)
Syracuse University (SU)
The College of New Jersey (TCNJ)
University of Puerto Rico - Mayagüez (UPRM)

UTRC Key Staff

Dr. Camille Kamga: *Director, Assistant Professor of Civil Engineering*

Dr. Robert E. Paaswell: *Director Emeritus of UTRC and Distin*guished Professor of Civil Engineering, The City College of New York

Herbert Levinson: *UTRC Icon Mentor, Transportation Consultant and Professor Emeritus of Transportation*

Dr. Ellen Thorson: *Senior Research Fellow, University Transportation Research Center*

Penny Eickemeyer: *Associate Director for Research, UTRC*

Dr. Alison Conway: *Associate Director for Education*

Nadia Aslam: *Assistant Director for Technology Transfer*

Nathalie Martinez: *Research Associate/Budget Analyst*

Tierra Fisher*: Office Assistant*

Bahman Moghimi*: Research Assistant;*
Ph.D. Student, Transportation Program

Wei Hao*: Research Fellow*

Andriy Blagay: *Graphic Intern*

TECHNICAL REPORT STANDARD TITLE PAGE

1. Report No.	2.Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle The Game-Theoretic National Interstate Economic Model: An Integrated Framework to Quantify the Economic Impacts of Cyber-terrorist Behavior		5. Report Date 12/12/2014 6. Performing Organization Code BUF
7. Author(s) Jiyoung Park		8. Performing Organization Report No. BUF-1
9. Performing Organization Name and Address University at Buffalo 05L Hayes Annex C 3435 Main St. Buffalo, NY 14214		10. Work Unit No. 11. Contract or Grant No. 49997-38-24 , DRTC-G-UTC02
12. Sponsoring Agency Name and Address University Transportation Research Center The City College of NY Marshak 910 137th Street and Convent Avenue New York, NY 10031		13. Type of Report and Period Covered Final, October 1, 2012 to March 31, 2014
15. Supplementary Notes		

16. Abstract

This study suggests an integrated framework to quantify cyber attack impacts on the U.S. airport security system. A cyber attack by terrorists on the U.S. involves complex strategic behavior by the terrorists because they could plan to invade an airport electronic system without any U.S. border or entry point. At the same time, any defending entity must consider the complex processes that may cause turmoil. The possibility of simultaneous threats from cyber attacks causes another difficulty for defending entities to secure their airports. This highlights the need for improved, integrated inter-governmental collaboration. Collaborative networking requires close inter-governmental coordination to overcome the risk of cyber-terrorist threats. Constructing a new model for strategic cyber-terror security requires a combination of both competitive and cooperative game situations in order to seek specific strategies against cyber-terrorism. Also, the airport shut-down would have ripple impacts throughout the domestic and international economies, which raises the necessity to analyze the impacts with a spatially disaggregate economic model. To combine both competitive and cooperative game situations with an economic impact model, this study suggest a Game Theoretic National Interstate Economic Model (G-NIEMO) framework. G-NIEMO identifies which airport may be most vulnerable in the event that an airport electronic system is subsequently shut-down. Based on the probabilistic costs of airport closure, the model provides the economic importance of cyber security by place of event and by type of industry. From G-NIEMO, equilibrium strategies for U.S. airport protection can be identified and a general guideline for the evaluation of resource allocations can be passed onto the U.S. government agencies.

17. Key Words National Security, Terrorism, G-NIEMO framework, Economic Impacts	18. Distribution Statement		
19. Security Classif (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No of Pages 29pages	22. Price

Form DOT F 1700.7 (8-69)

Disclaimer

Acknowledgment

The author wishes to acknowledge the intellectual comments from Professors Peter Gordon (University of Southern California) and Jason Levy (Virginia Commonwealth University). Also, the author appreciates Professors Shambhu Upadhyaya, Raghav H. Rao, Jun Zhuang and Changhyun Kwon at the University at Buffalo and Professor Minsu Son at Seoul National University for their valuable comments.

Abstract

This study suggests an integrated framework to quantify cyber attack impacts on the U.S. airport security system. A cyber attack by terrorists on the U.S. involves complex strategic behavior by the terrorists because they could plan to invade an airport electronic system without any U.S. border or entry point. At the same time, any defending entity must consider the complex processes that may cause turmoil. The possibility of simultaneous threats from cyber attacks causes another difficulty for defending entities to secure their airports. This highlights the need for improved, integrated inter-governmental collaboration. Collaborative networking requires close inter-governmental coordination to overcome the risk of cyber-terrorist threats. Constructing a new model for strategic cyber-terror security requires a combination of both competitive and cooperative game situations in order to seek specific strategies against cyber-terrorism. Also, the airport shut-down would have ripple impacts throughout the domestic and international economies, which raises the necessity to analyze the impacts with a spatially disaggregate economic model. To combine both competitive and cooperative game situations with an economic impact model, this study suggest a Game Theoretic National Interstate Economic Model (G-NIEMO) framework. G-NIEMO identifies which airport may be most vulnerable in the event that an airport electronic system is subsequently shut-down. Based on the probabilistic costs of airport closure, the model provides the economic importance of cyber security by place of event and by type of industry. From G-NIEMO, equilibrium strategies for U.S. airport protection can be identified and a general guideline for the evaluation of resource allocations can be passed onto the U.S. government agencies.

* The author wishes to acknowledge the intellectual comments from Professors Peter Gordon (University of Southern California) and Jason Levy (Virginia Commonwealth University). Also, the author appreciates Professors Shambhu Upadhyaya, Raghav H. Rao, Jun Zhuang and Changhyun Kwon and Post-doctoral scholar Minsu Son at the University at Buffalo for their valuable comments.

I. National Security, Terrorism, and Economic Impacts

U.S. border security has been dramatically tightened since September 11, 2001. According to U.S. Customs and Border Protection (CBP), its "top priority is to keep terrorists and their weapons from entering the United States" (CBP, 2008). Enhanced tightness of the U.S. border for national security has been mostly implemented to prevent physical invasions. Unfortunately, it appears that the Department of Homeland Security (DHS) may not plan and manage possible physical invasions through the U.S. borders effectively (Tirman, 2006), and this is much clearer in the case of cyber attacks.

Also, many studies have focused only on evaluating physical terrorist attacks that may potentially cause severe economic consequences stemming from infrastructure damage and business interruption in the areas affected in terms of the direct and indirect impacts on the economy (Park, 2008; Park et al. 2007; Richardson et al. 2007; Gordon et al., 2007). Major U.S. airports have been provided useful information on the plausible catastrophes by those studies, and public and private industry sector decision-makers could also be advised to evaluate their expenditures to mitigate and respond to an emergent event. However, such economic impact analysis studies have been limited to measuring physical economic damages under some restricted assumptions and scenarios without considering cyber events and probability of or resilient process after an event.

A cyber attack by terrorists on the U.S. airports involves complex strategic behavior by them because they could plan to invade an airport electronic system bypassing any U.S. border or entry point. At the same time, any defending entity must consider the complex processes that may cause turmoil. The possibility of a threat from simultaneous cyber attacks causes another difficulty for defending entities to secure their airports. This highlights the need for improved, integrated collaboration between local governments, between local and federal governments, even and/or between countries involved in this type of attack. Collaborative networking, connected domestically and internationally in terms of governmental cooperative integration, requires close inter-governmental coordination to overcome the risk of cyber-terrorist threats. For example, if cyber terrorists are able to successfully invade one U.S. airport information system, this could cause a problem in the operational software and database that contain valuable information. The one event could affect not only the entire region that the airport is located in, but also other domestic and international airports connected to that airport. Air transport substantially contributes to the global economy up to $1,540 billion and 33.3 million jobs (Oxford Economics, 2009). Constructing a new model for strategic cyber-terror security requires a combination of both competitive and cooperative game situations in order to seek specific strategies against cyber-terrorism. Also, the airport shut-down would have ripple impacts throughout the local and domestic economies, which raises the necessity to analyze the impacts with a spatially disaggregate economic model.

Suggesting a new framework to quantify possible economic impacts of a breached strategic airport security requires combining the probability of cyber attacks with consequent economic impacts. A new probabilistic economic impact model suggested in this study can provide estimates of differentiated economic impacts by region and by industry. By combining both competitive and cooperative game situations with an economic impact model, this study proposes a framework of “Game Theoretic” extension of our National Interstate Economic Model (NIEMO) (see selective

NIEMO contributions at Park, 2008; Park et al., 2007; 2008; 2009a; 2011; 2012). The G-NIEMO can be used to identify which airport may be most vulnerable in the event that an airport electronic system is subsequently shut-down. Based on the probabilistic costs of airport closure, the model provides the economic importance of cyber security by location of event and by type of industry. Indeed, the results of this research will advance our understanding of how uncertain cyber attacks affect the real economies of the U.S. From G-NIEMO, equilibrium strategies for U.S. airport protection against cyber terrorists can be identified and a general guideline for the evaluation of resource allocations can be passed onto the U.S. government agencies. Finally, it is expected that this study will provide to a basis for communication among policy makers, the general public and local economic activity entities associated with aviation security and policy.

Hereby, the next section in this study discusses both competitive and cooperative strategic behaviors in a game theoretic situation and a spatially disaggregated economic impacts model for the U.S. The third section introduces an integrated modeling framework for strategic cyber-terror security that combines both competitive and cooperative game situations with the spatially disaggregate economic model applied for the measurement of probabilistic economic costs. With a brief summary and some discussions to be added in new research, this study concludes.

II. Game Theory and Economic Impact Model

In summer 2011, the Indira Gandhi International (IGI) Airport's Terminal 3 in Delhi experienced a simple technical failure in the Common Use passengers Processing System (CUPPS) due to a virus attack on the system as per the Central Bureau of Investigation (CBI) of India; While the system was down and switched to manual check-in for a half day, about 50 flights were delayed for 15 to 20 minutes (Kakkar, 2011). More recently, four months ago, the U.S. experienced a cyber attack on airport information systems via malware insertion that might have caused serious malfunctions on diverse control systems from air traffics to air conditioning pipes on airplanes (Doglow, 2012). The experience warns us that cyber attacks do not mean a simple threat to airport control systems, but may cause serious physical disruptions on the targeted airport and result in the airport shutdown as a result of the disruptions (AFP, 2010).

There is no doubt that analyzing the cost-effectiveness of efforts to heighten border security is meaningful to lessen possible physical attacks. Hence, it requires not only applying benefit-cost analysis for each border but also understanding the defender's strategy to determine which border may be most vulnerable from the terrorists' perspective. Even more seriously, when considering cyber attacks that disable or delete critical infrastructure system data (Tafoya, 2011), the strategic game situation is much clearer for the case of cyber-terror attacks. A physical attack planned by terrorists to the U.S. usually starts with complex strategic behaviors of terrorists because they may intend to cross any U.S. border. At the same time, a defensive entity should consider the complex process that may cause catastrophic results once it would happen. However, if cyber terrorists are able to successfully invade one of the U.S. airport systems to causing a problem to operational software that controls all airplane schedules, the one event may affect not only the entire region where the airport is located, but also other domestic and international airports that are connected to that airport. The airport shut down will make a ripple effect throughout the domestic and international economy.

Indeed, in the current technologically advanced era, the following fundamental questions need to be raised in a cyber-terror policy analysis procedure: how can we effectively analyze the defensive scientific and technological improvement with the terrorist strategy that has been also intelligent along with modern technology innovations? If we consider both economic damage and risk probability, how can we advance an analysis tool that considers them effectively and simultaneously? Part of the answer involves a clearer understanding of the procedure in the cyber-attacks and of the economic impacts of the cyber-terror events. It requires the analysis of strategic behaviors among groups involved in cyber attacks. Also, after an event has occurred, the costs estimated need to consider additional impacts that extend from direct impacts occurred in airport system disruptions. The estimated costs to the counter-terrorism are usually applied for policy benefits that hinge on the economic losses which could be prevented and need to be extended to measuring other regional losses.

It is certain that the U.S. anti-terrorism policy has been tremendously relying on the improvement of its scientific and technological assets. At the same time, the modern scientific and technological innovation has been advancing the strategic options that terrorists may consider for their invasion to the U.S. Certainly, there are massive records of recent cyber-attacks on modernized scientific transportation sectors and the number of attacks are increasing, indicating the more computerized in transportation systems, the more potentially vulnerable to be attacked by the intelligent cyber-hackers. For example, cyber-hackers may substantially disable automobile and subway control systems because modern transportation network systems are pervasively computerized and may be attacked without spatial and temporal restriction (Koscher et al., 2010; Ignelzi, 2012).

It is clear that more air, water and ground networks will be affected by cyber-terrorists in the future. Further, it is more vulnerable and risky when cyber-attacks domestic and/or international infrastructure simultaneously because the visible and invisible threats have been increasing dramatically with extremely easy access to the internet. The simultaneous attacks highlight the need for improved, integrated collaboration between local governments, between local and federal governments, and/or between countries involved in the attacks. The collaborative networking, connected horizontally and vertically in terms of governmental cooperative integration, requires close inter-governmental coordination to overcome the risky cyber-terrorist threats.

Traditionally game theory has been widely applied to analyze a competition, non-cooperative interactive decision process especially since 1970. Based on the strategies evolved from "the selfish gene," the competitive, evolutionary dynamic game process is more realistic in finding a best agreement under the restricted conditions (Benkler, 2011b). Unfortunately, the agreement found from the competitive process is unstable and fragile to keep the balance because it is more effective to problem identification or diagnostic process. However, a public solution suggested requires public support that satisfies interest groups and organizations. Also, public policy process requires this type of public solution to a problem which is identified publically (McCain, 2009). This type of process suggests publically enforceable agreements. A game theory tool applicable to the collaborative interaction provides what various mechanisms can encourage cooperating and overcoming a disastrous risk (Benkler, 2011a; Nowak and Highfield, 2011). As Benkler (2011b) is clearly addressing, the cooperation, collective interdependent actions among groups are more effective and play a more important role to a risky disaster than the fittest action plan via competitive and non-cooperative strategic behavior process because they receive public agreements.

How can the cooperative collective action be applicable to maintaining an unarmed civilian society threatened by cyber-terrorist attacks? The civilian society pursues to reach new levels that improve cyber security and reduce economic damages with the rapid growth of the internet that uncovers spatial and temporal restrictions to access established, developed societies. A strategic approach to modeling cooperative and collective actions among governments, as well as the complex competition actions between hackers and governments, requires an integrated, structural super-cooperation in order to include those horizontally and vertically connected but adverse actions. Panels in Figure 1 demonstrate this integrated structure of complex behavioral actions in cyber-terrorism.

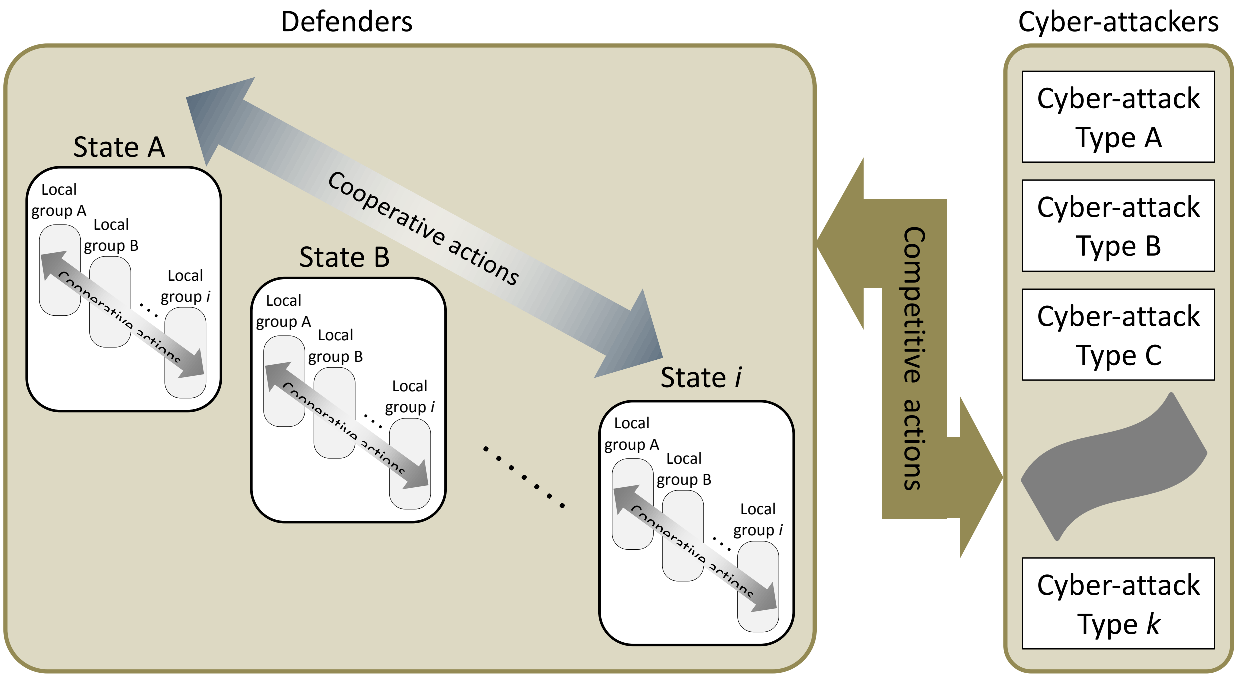


Figure 1. The hierarchical and horizontal structure of complex behavioral actions in cyber-terrorism

II-1. Competitive and Cooperative Game Process

Competitive game theory is widely applied to the study of strategic interactions between attackers and a defending government (Sandler and Arce M., 2003). Unlike natural disasters, terrorists are intelligent and adaptive; they may anticipate where the current border security measures are weak and utilize diverse, illegal network channels to transport money, weapons, and/or personnel. For example, if considering border security of one country from physical terrorists' invasion that explains the competitive strategy of national security responding to terrorist attacks, the game theoretic situation begins with behavioral strategy that terrorists may intend to cross any U.S. border. As a defender, the U.S. may respond to the terrorists' possible attacks when making defensive decisions of, e.g., how many resources need to be allocated to prevent any possible violation by terrorists (Zhuang and Bier, 2007). Once resolving the competitive game probabilities, by connecting to an economic impact model that is described in Section II-2 as a spatially disaggregate macro-economic model of the U.S., the U.S. federal policy makers can benefit from suggestions on which borders should be considered for protection force. Specifically, it is expected that the effectiveness of the U.S.CBP can be significantly enhanced by the findings suggested with the competitive approach, because it eventually delivers a simulated probabilistic economic costs package that will be used by the Department of Homeland Security (DHS) and for other scholars involved in border security. The study conducted by Zhuang and Bier (2007) analyzed such strategic competitive interactions between terrorist groups and the defender using game-theoretic models.

While the game-theoretic view of this physical invasion by terrorists is a complex but competitive situation (Sandler and Arce M., 2003), the game view is not considering how local border securities collectively cooperates to protect the U.S. borders or how national governments cooperate internationally to protect their important infrastructures from the possible terrorists' attack. Furthermore, several innovative approaches to deterring possible attackers have been suggested (see for example Frey and Luechinger, 2003; 2004; Perrow, 2006; Keohane and Zeckhauser, 2003), it is rare to find the strategic allocation of defensive resources improving border security by reducing the expected costs of a potential attack. Therefore, cooperative, as well as competitive, strategies and economic impact analysis measuring economic costs should be incorporated into a model in order to evaluate current cyber-terror security and simulate the optimal future allocations of international and federal resources to the security of infrastructure systems. The distinctive feature to combine the strategic situation of terrorists with an economic impact model is suggested in Figure 2. The lower panels demonstrate how economic impact model can be combined with the complex game situation in the upper panels. The total probabilistic economic impacts will provide another signal to defenders and cyber-attackers and the process repeats until reaching equilibrium. The detailed process is explained in Section III.

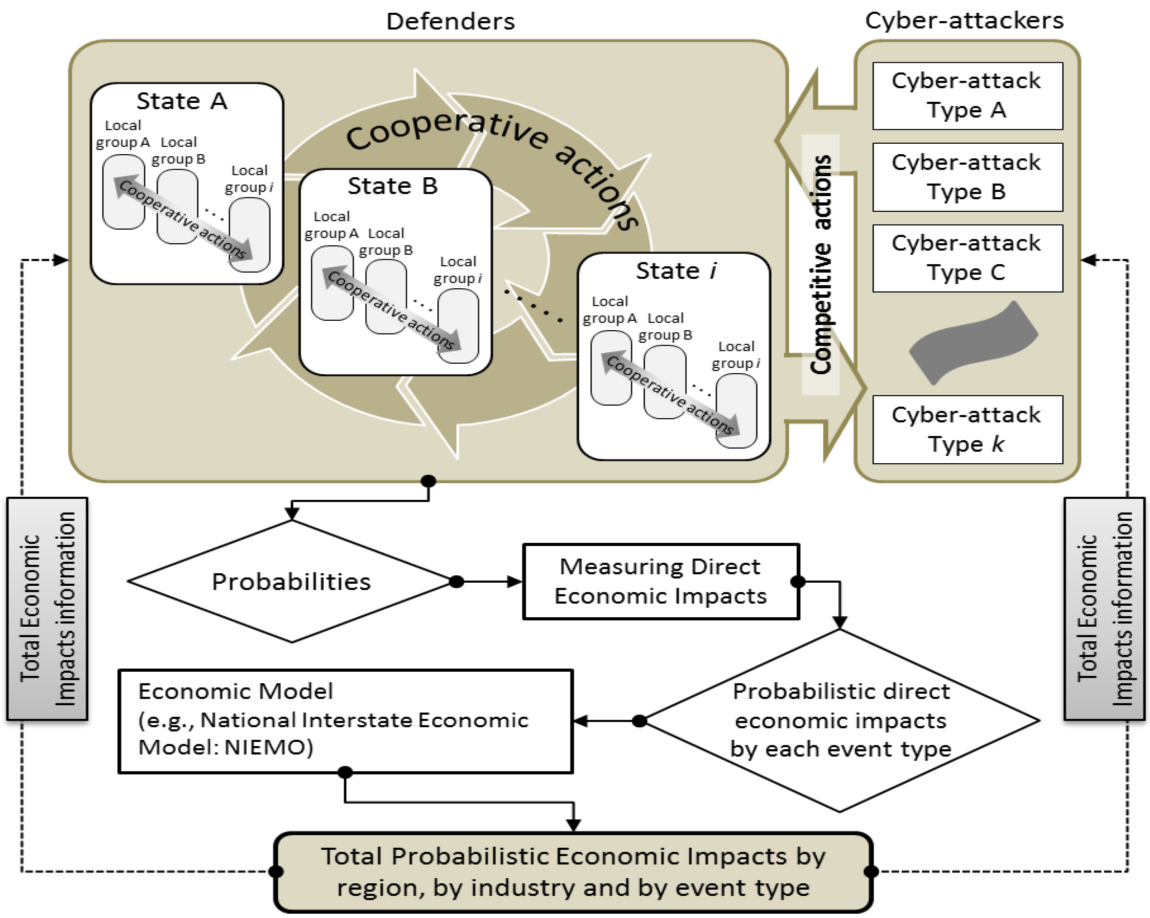


Figure 2. Procedure to Measure Economic Impacts via an Integrated Game Theoretic Economic Impact Model

II-2. National Interstate Economic Model (NIEMO)

Many economists and regional scientists have applied input-output (I-O) or computable general equilibrium (CGE) for analyzing the socioeconomic impacts of disruptions resulting from diverse disasters. The traditional, one region type of I-O models that Isard demonstrated in 1951 are not enough to apply for capturing the interlinked effects among regions. To measure the interregional impacts of terrorist attacks on one country, the economic links among sub-national areas should be specific. Instead of surveying all interregional economic connections of which costs are huge, Chenery (1953) and Moses (1955) had demonstrated a relatively simplified multiregional input output model (MRIO) framework in response to the "ideal interregional model" suggested by Isard (1951, 1960), which can be an alternative to measuring the interregional economic connections based on interregional trade flows to avoid some problems associated with excessive spatial aggregation; When an I-O model is spatially aggregated, it especially loses spatial information, because a terrorist attack may impact negatively on the targeted area but may have positive economic boosts to another. Because most politicians have keen interests in their local constituencies, thereby, a state-to-state economic model may substantially contribute to providing such information.

The National Interstate Economic Model (NIEMO), an economic multiregional input output (MRIO) model for the 50 states and the District of Columbia (D.C.) of the U.S., is the first operational MRIO model of the U.S since 1990 (Park et al., 2007). Most studies that apply NIEMO have focused on regional and national economic impact measures stemming from diverse man-made and natural disasters and suggest plausible, public policy alternatives. As a primary tool of application to regional and national security problems, NIEMO has been applied with the combination of various econometric methods to quantify the costs of national security.

The main reason that this MRIO type model for the U.S. has not been operational stems from the non-existence or rarity of useful interstate trade data. Even though intraregional interindustrial data and interregional trade data must be comparable and compatible, the currently available commodity-based trade flows data between states are only sporadically available and difficult to connect the sector system to other U.S. industrial sector systems such as North American Industrial Sector Code (NAISC). Building an operational multiregional input-output model (MRIO) that includes all the states in the U.S. have been in trouble because it required highly detailed interstate trade flow data by industry type. Due to the problematic data, only a few MRIO-type models for the U.S. have been constructed, which include the year of 1963 based MRIO for 51 regions and 79 sectors demonstrated by Polenske (1980) and the year of 1977 based MRIO for 51 regions and 120 sectors published by Jack Faucett Associates (1983). The latter was updated and reported in 1988 (Miller and Shao, 1990).

NIEMO basically applied Commodity Flow Survey (CFS) data to estimate interstate trade flows (Park et al., 2009a) and IMPLAN data (from the Minnesota IMPLAN Group; MIG, Inc.) for interindustrial transaction flows by state. After discontinuation of the U.S. Commodity Transportation Survey Data on inter-regional trade flows for some years, the Bureau of Transportation Statistics (BTS) released CFS data every five years since 1993; however, these CFS data are not reporting complete interstate trade flows. As demonstrated in Figure 3, based on the currently available CFS data, Park et al. (2009a) estimated complete trade flow data and updated to a target period that matches IMPLAN data sets by applying an Adjusted Flow Model

(AFM) and a Doubly-constrained Fratar Model (DFM). The approach necessarily requires creating conversion tables that reconcile the sectors between CFS and IMPLAN and detailed procedural bridges are explained in the study of Park et al. (2009a). While the current NIEMO relies on 1997 CFS and 2001 IMPLAN data, the systematic approach that is still operational is able to update. The current version of NIEMO tried to reconcile different sector definitions and classifications of the commodities among multiple data sources and used a new commodity sector system of 29 commodity and 18 service sectors. Park and Gordon (2005) demonstrated the interstate trade flows and the trade flows between the U.S. states and the rest of world are reliable and even more important to provide the spatial information than to provide detailed sectoral information.

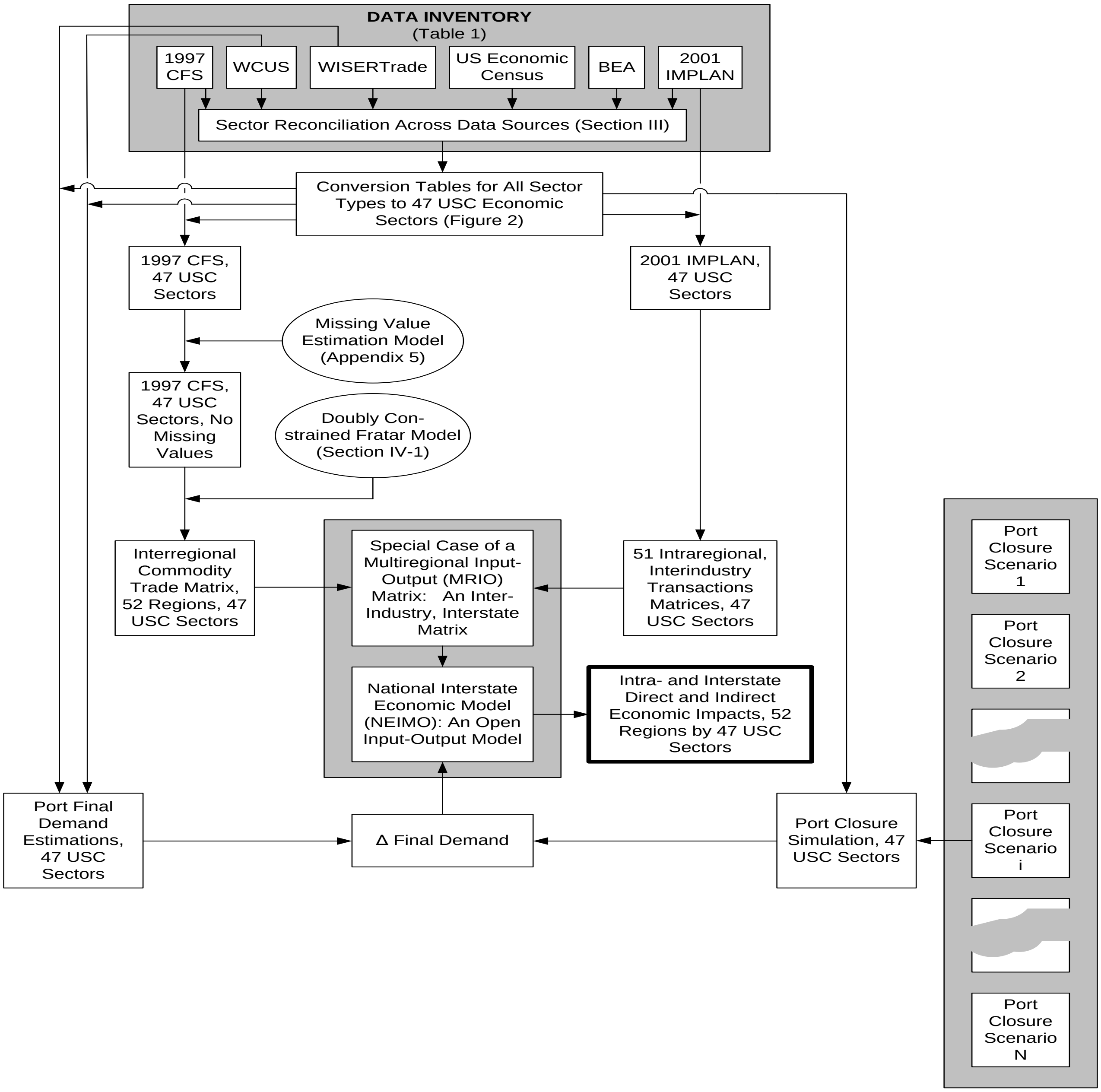


Figure 3. NIEMO Modeling and Development process

Source: Park et al. (2007), p.213, Simulating The State-by-State Effects of Terrorist Attacks on Three Major US Ports: Applying NIEMO (National Interstate Economic Model)

Applying NIEMO to various empirical studies includes hypothetical terrorist attacks that were already published in several venues (Park et al., 2008; Park, 2008; Richardson et al., 2007a). Also, NIEMO has applied for diverse natural disaster studies (Park et al., 2012; Park, 2012) and all U.S. borders closure when international avian influenza epidemic occurs (Gordon et al., 2009). Table 1 summarizes the various economic impacts studies that NIEMO has been applied.

NIEMO has been evolving. It has been extended to the sub-state level (Southern California Interregional Input-Output; SCI-IO) and temporally (Flexible NIEMO: FlexNIEMO), combined with transportation network system (Transportation network NIEMO: TransNIEMO), and environmental (EnviNIEMO) models to address local and dynamic issues in a country. The extended NIEMO may investigate the magnitudes and policy implications of negative economic impacts resulting from disruptive events, including losses of infrastructure services (notably transportation) due to natural or man-made disasters at various regional levels. The importance of maintaining our social, economic, and community development systems in an era of new uncertainties from possible disasters involving climate change or terrorist attacks may be accurately, easily addressed by NIEMO and its extensions. Certainly terror prevention programs that are accomplished at all levels of government should closely connect national prevention programs with many localized constituencies to be politically supported. Also, aggregate cost analysis may be incomprehensible to deliver localized effects due to the cancellation of local impacts on each other.

Table 1. Various Economic Impacts Studies Using NIEMO

Nature of Disruption	Targets	Reason for Economic Impact	Total Economic Impacts ($M)	Base year, Duration, and Model	Citations	Note
Explosives	LA/LB, Houston, and NY/NW	Ports shut-down	23,258	2001, one-month, and demand-driven NIEMO	Park et al., 2007	Direct/Indirect state-by-state impacts
Dirty-bomb	LA/LB	Ports shut-down	26,905	2001, one-month, and supply-driven NIEMO	Park, 2008.	Direct/Indirect state-by-state impacts
9/11	U.S. Airports	Losses of air-passengers	214,347 ~420,455	Sep. 2001 ~ Aug. 2003, 2 years, and IMPLAN IO model	Gordon et al., 2007	Direct/Indirect/Induced impacts of the U.S.
Mad-cow-disease	U.S. Bovine animal	Foreign exports closing	13,681	Dec. 2003 ~ Apr. 2005, 15 months, and demand-driven NIEMO	Park et al., 2007.	Direct/Indirect state-by-state impacts
Explosives	13 U.S. theme parks	Losses of consumers	20,747 ~ 24,921	2004, 18 months, and demand-driven NIEMO	Richardson et al., 2007a.	Direct/Indirect state-by-state impacts
Hurricanes Katrina and Rita	U.S. oil-refinery industries	U.S. oil price increase	1,537	2005, 4 months, and price-sensitive supply-driven USIO	Park, 2012	Direct/Indirect U.S. impacts
Hurricanes Katrina and Rita	PADD III	Disruption of Oil-refinery industries	4,849	2005, 13 months, and supply-driven FlexNIEMO	Park et al., 2012.	Direct/Indirect state-by-state and month-to-month impacts
International avian influenza epidemic	Loss of Air passengers, U.S. seaports closing, loss of cross-border shopping, loss of legal and illegal labors	U.S. border closures	1,734,075 ~5,408,796	2001, one-year, and demand- and supply-driven USIO and NIEMO.	Gordon et al., 2009.	Direct/Indirect state-by-state or U.S. impacts
Hurricanes Katrina and Rita	Louisiana customs district	Seaports shut-down	44,374	Aug. 2005 ~ Mar. 2006, 8 months, and demand- and supply-driven NIEMO.	Park, et al., 2008b.	Direct/Indirect state-by-state impacts

III. Game Theoretic NIEMO: G-NIEMO

The distinctive feature of this study is to incorporate the strategic situation of terrorists by combining game theory with NIEMO. Constructing a new model for strategic cyber-terror security requires a combination of both competitive and cooperative game situations with a spatially disaggregate economic model; the latter requires expected input costs in order to estimate total costs. As demonstrated in Figure 2, the general conceptual approach to calculating the economic costs of cyber-terror attacks is to multiply the success probability of a cyber-terrorist invasion to important transportation infrastructure, e.g., airports and the corresponding cost if those airports were subsequently closed. By constructing a metric table of the probabilistic costs for all airports considered in the U.S., we can evaluate which airport may be most vulnerable in terms of cyber security. The dual-methodology combined model, a game-theoretic model and NIEMO, will generate a new integrated model that we call the Game Theoretic National Interstate Economic Model (G-NIEMO).

G-NIEMO as a game-theoretic economic impact model provides probabilistic economic costs for each airport or multiple airports if targeted simultaneously. The model starts by analyzing the probability of each or multiple airports in the U.S. being attacked, in conjunction with the application of game theoretic model. The direct cost of closure of one or multiple airports is then estimated with disruption scenario development. The product of the probability and the direct cost will then be used as input to NIEMO. Via NIEMO, the probabilistic total economic cost (by sector, by region and by scenario) of those airports closed will be estimated. Finally, the total economic losses will be provided to defenders and cyber-attackers as new information and new economic impacts will be measured. Detailed procedures for the approach are as follows.

Step I: Modeling Competitive (Defender and Attacker Strategic) and Cooperative (Defender and Defender Strategic) Interactions

For one or multiple airports, the U.S. government chooses the level of defensive investment in terms of finance, equipment, and/or personnel. An attacker observes (or anticipates) the defender's choices, and then chooses the best response (or the probability of launching an attack against each or multiple airports). While competitive strategic interactions at this level may apply different forms of conflict success functions in order to estimate these probabilities (Skaperdas, 1996; Hausken, 2004), another form of function requires local governmental cooperative interactions as well as international cooperative interactions to collectively defend the cyber-terrorist attacks. For example, simultaneous cyber-attacks are plausibly made for John F. Kennedy (JFK) International Airport in the U.S. and Toronto Pearson International Airport in Canada, and it is extremely important to share any piece of information to defend the economic activities of these two megacities, most of which are served by the main hubs. Furthermore, JFK airport is tightly connected with other airports in the U.S. which will disrupt U.S. economic activities, and hence, local cooperative strategic interactions are critical to prevent the cyber-violation. This step requires the analysis on competitive and cooperative strategic behaviors.

Step II: Estimating Direct Costs

For individual and cooperative possible defender strategy corresponding to the cyber-attackers, hypothetical and/or actual historical measures of direct costs for the successful invasion that may occur should be estimated. Diverse historical data can be found from sources such as the Bureau of Economic Analysis (BEA), Office of Travel and Tourism Industries (OTTI), the Travel Industry

Association (TIA), the Bureau of Transportation Statistics (BTS), the Bureau of Labor Statistics (BLS), etc. and combined with hypothetical invasion scenarios. The collected data will be used to calculate the direct cost to airport closure and provide numerical experimental results to measure the importance of each airport.

Step III: Estimating Probabilistic Direct, Indirect and Total Costs

Based on the probability of a successful attack and the direct cost for one or multiple airport closures, a panel graph can be drawn as suggested in Figure 4. It demonstrates where each airport fits in each panel.

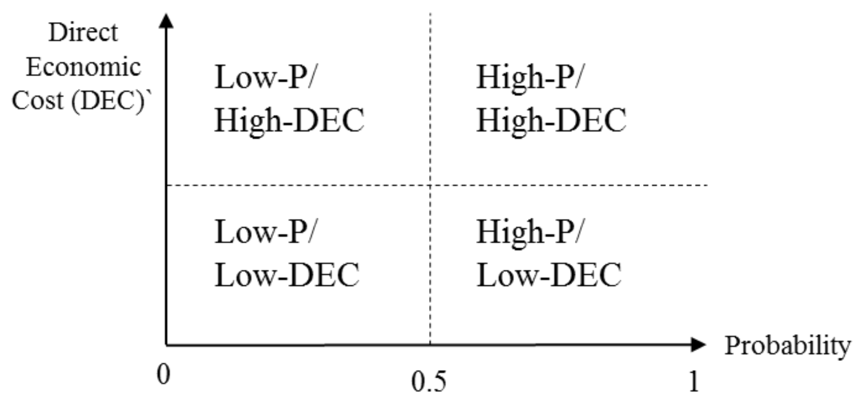


Figure 4. Probability and Direct Economic Cost (P/DEC) Panel for Cyber-terror Invasion

It is clear that high probability (High-P) and high direct economic cost (High-DEC) airports, whether it is collectively or individually measured, need to be first considered for the U.S. government investment. While it is clear to least consider for the airports located in the panel of low probability (Low-P) and low direct economic cost (Low-DEC), it is wise to compare a panel of Low-P/High-DEC and a panel of High-P/Low-DEC airports. The product of the probability of a successful attack for an airport will be calculated to verify the possible direct cost resulting from the airport closure. Aggregating the probabilistic direct costs of each airport by state provides expected direct damages that each U.S. state may experience. The expected, probabilistic direct costs by state will be used to estimate indirect and total potential costs for the U.S., considering inter industrial and interregional economic relations that each airport supports via NIEMO.

Step IV: Evaluating Equilibrium Probabilistic Impacts and Vulnerable Ranking Metrics

The estimated total impacts will be used for additional information for cyber-terrorists and defenders. Both players will receive this information in deciding their equilibrium strategies, which result in an updated estimation of total economic impacts as suggested in the right and left bent-up arrows of Figure 2. Such feedback process will repeat until they reach equilibrium. Finally, the equilibrium total impacts will be used for constructing a vulnerable ranking score metric that demonstrates which airports are most vulnerable from cyber attacks. The vulnerability metric may be further analyzed by industry type, by scenario, and by geographical boundary. The provided information will be used to determine which state and airport should be first considered for the distribution of defensive resources available in the U.S.

Step V: Evaluating G-NIEMO

From G-NIEMO, equilibrium strategies for U.S. airport protection will be computed. To evaluate the G-NIEMO reliability, it is suggested to compare the computed equilibrium strategies from G-NIEMO to those computed from traditional game-theoretic models, as well as the real data. The results will be used to evaluate the G-NIEMO approach and may eventually help the resource allocations by the U.S. government.

IV. Conclusions

Aviation deterrence is crucial in fighting cyber-terrorism. Aviation security from cyber invasion is especially critical because airport network is the heart to support economic activities for human and freight rapid movements which are necessary for the other industrial activities. However, in many cases we have been observing that cyber-terrorists are superior to the governmental cyber security for transportation network system (Richardson et al., 2007b). As Poole (2007) suggested, the sizable variation in the U.S. airports, one of three basic flaws of the Transportation Security Administration (TSA) in aviation security, may not be controlled by the TSA's centralized approach.

To effectively prevent vulnerable and risky airports exposed to cyber-terrorists, therefore, it is important to improve collaboration between local and federal entities and integrate local strategies on cyber-terrorism that may simultaneously attack the U.S. airports. The collaborative strategy integrates the U.S. aviation security network, horizontally and vertically connecting federal, local, and other non-profit cooperative entities. Modeling this cooperative strategy should be integrated to the traditional, competitive game process to solve such complex behavioral action strategies.

By combining the probability of invasion with economic impacts, the G-NIEMO framework that quantifies the economic impacts on the strategic infrastructure security may differentiate economic impacts by event place and by target industry. From G-NIEMO, equilibrium strategies for U.S.

airport protection can be measured. Comparing the computed equilibrium strategies from G-NIEMO with those computed only by traditional game theoretic models may provide a general guide on the evaluation of resource allocations by U.S. governments.

One issue to be considered is resilience; Many scholars agree that it refers to the defensive capacity to diminish the maximum potential impacts at any given point in time after a terrorist attack and the ability to recover as quickly as possible (Park et al., 2011; 2008; Mcdaniel et al., 2008; Rose, 2004; 2007; Adger, 2000). One major way in which the airport resilience from a cyber-terror attack may take place is when the airport resumes its operation after some repair recovering the original schedule takes place and before airplanes that use the airport persistently change to near airports whose services and benefits are not very different. According to Park et al. (2009b) and Rose et al. (2009), experience with the 9/11 attack as well as most physical disasters indicates that the economy of the U.S. and states near New York had substantial resilience. Unfortunately, different from factory operation to produce goods, the air or water port operational services are not able to recapture the lost services.

Certainly, it is possible to measure some portion of the lost production in an economy from physical disruption by applying a fixed parameter (FEMA, 1997; Rose and Lim, 2002; Rose et al., 2007) or a relaxed, functionalized parameter (Park et al., 2011) for each of several industrial sectors, but most operational service sectors of infrastructure are almost zero to the resilience action. The resilient application to a cyber-terror attack may be essential to rather accurately estimating the business interruption that is indirectly affected by infrastructure service malfunctionality. However, a general framework that addresses national and international transportation network security prevented from cyber-attacks still requires the initial suggestion of combining multidirectional, complex game theoretic situations with a spatially disaggregate economic model which can trace local economic activities. The remaining resilient discussion should be investigated in a future research.

References

Adger, W. Neil, 2000, Social and ecological resilience: are they related? *Progress in Human Geography* 24(3): 347-364.

AFP, 2010. Airliners Fly in Face of Cyber Attack Scares: What would happen if all those screens tracking all those flights suddenly went blank? November 3, 2010. Available at http://news.discovery.com/tech/cyber-attack-air-traffic.html (accessed December 2012).

Benkler, Y., 2011, *The Penguin and the Leviathan: The Triumph of Cooperation Over Self-Interest*, Crown Business.

Benkler, Y., 2011b, The Unselfish Gene, *Harvard Business Review*, 89 (7-8):76-85.

CBP. 2008. About Border Security. available at http://www.cbp.gov/xp/cgov/border_security/bs/ (accessed September 2008)

Chenery, H.B., 1953, Regional Analysis, in *The Structure and Growth of the Italian Economy*, edited by H.B. Chenery, P.G. Clark and V.C. Pinna, US Mutual Security Agency, Rome: 98-139

Doglow, M., 2012. Cyberwars Reach a New Frontier: the Airport, August 15, 2012. Available at http://www.businessweek.com/articles/2012-08-15/cyber-wars-reach-a-new-frontier-the-airport (accessed December 2012).

Federal Emergency Management Agency (FEMA), 1997, *HAZUS®99 Earthquake Loss Estimation Methodology: User's Manual*.

Frey, B. S., S. Luechinger. 2003. How to fight terrorism: Alternatives to deterrence. *Defence Peace Econom*. 14(4) 237–249.

Frey, B. S., S. Luechinger. 2004. Decentralization as a disincentive for terror. *Eur. J. Political Econom*. 20 509–515.

Gordon, P, JE Moore, II, JY Park, and HW Richardson, 2007, The Economic Impacts of a Terrorist Attack on the US Commercial Aviation System, *Risk Analysis*, 27 (3): 505-512.

Gordon, P., J.E. Moore II, J.Y. Park, and H.W. Richardson. 2009. The Economic Costs of Border Closure: A State-by-State Analysis. p341-374, in HW Richardson, P Gordon and JE Moore II, eds, *Global Business and the Terrorist Threat* Cheltenham: Edward Elgar

Hausken, K., 2004. "Mutual Raiding of Production and the Emergence of Exchange," *Economic Inquiry*, Oxford University Press, 42(4): 572-586.

Ignelzi, L., 2012, *Hackers manipulated railway computers, TSA memo says*, http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/, accessed on June 10, 2012

Isard, W., 1951, Interregional and Regional Input-Output Analysis: A Model of a Space Economy, *Review of Economics and Statistics*, 33: 318-328

Isard, W., 1960, *Methods of regional analysis: An introduction to regional science*, The MIT Press

Jack Faucett Associates, INC, 1983, *The Multiregional Input-Output Accounts, 1977: Introduction and Summary, Vol. I (Final Report)*, prepared for the US Department of Health and Human Services, Washington

Kakkar, M., 2011. CBI believes cyber attack led to IGI airport's technical problems in June, September 25, 2011. Available at http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710 (accessed December 2012).

Keohane, N.O. and R.J. Zeckhauser. 2003. The Ecology of Terror Defense. *J. Risk Uncertainty*. 26 201-229

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In D. Evans and G. Vigna, editors, *IEEE Symposium on Security and Privacy*. IEEE Computer Society, May 2010.

McCain. R. A., 2009, *Game Theory and Public Policy*, Cheltenham: Edward Elgar.

McDaniels, T., S. Chang, D. Cole, J. Mikawoz, and H. Longstaff. 2008. "Fostering Resilience to Extreme Events Within Infrastructure Systems: Characterizing Decision Contexts for Mitigation and Adaptation," Global Environmental Change 18(2): 310-318.

Miller, R.E. and G. Shao, 1990, Spatial and Sectoral Aggregation in the Commodity-Industry Multiregional Input-Output Model, *Environment and Planning A* 22: 1637-1656.

Moses, L.N., 1955, The Stability of Interregional Trading Patterns and Input-Output Analysis, *American Economic Review*, 45: 803-832

Nowak, M. and R. Highfield, 2011, *SuperCooperators: Altruism, Evolution, and Why We Need Each Other to Succeed*, Free Press.

Oxford Economics, 2009. *Aviation: The Real World Wide Web*. Onward Publishing, Inc.

Park, J Y, P Gordon, J E Moore II, H W Richardson, S Kim, and Y Kim, 2008b, “Estimating the State-by-State Economic Impacts of Hurricane Katrina,” p147-186, in HW Richardson, P Gordon and JE Moore II, eds, Natural Disaster Analysis after Hurricane Katrina Cheltenham: Edward Elgar

Park, J.Y. 2008. The Economic Impacts of a Dirty- Bomb Attack on the Los Angeles and Long Beach Port: Applying Supply-driven NIEMO (National Interstate Economic Model). *Journal of Homeland Security and Emergency Management*. 5(1)

Park, J.Y., C.K. Park, and S.J. Nam, 2006, The State-by-State Effects of Mad Cow Disease using a new MRIO model, Paper presented at 2006 American Agricultural Economic Association (AAEA) Annual Meeting, Long Beach, CA, USA, July 23-26.

Park, J.Y., Gordon, P., J. E. Moore II, and H.W. Richardson. 2008. The State-by-State Economic Impacts of the 2002 Shutdown of the Los Angeles-Long Beach Ports. *Growth and Change*, 39 (4) 548-572.

Park, J.Y., P. Gordon, J. E. Moore II, and H. W. Richardson, L. Wang, 2007. Simulating The State-by-State Effects of Terrorist Attacks on Three Major U.S. Ports: Applying NIEMO (National Interstate Economic Model). in H.W. Richardson, P. Gordon and J.E. Moore II, eds. *The Economic Costs and Consequences of Terrorism*: 208-234. Cheltenham: Edward Elgar.

Park, J.Y., P. Gordon, Y.K. Kim, J.E. Moore II, and H.W. Richardson, 2012, The Regional Economic Impacts of Hurricanes Katrina and Rita on Oil and Gas Refinery Operations in the Gulf of Mexico: Applying a Flexible Multi-regional Input-Output Model. Under-review at *Group Decision and Negotiation*.

Park, J.Y.; P. Gordon; E. Jun; J.E. Moore II; and H. W. Richardson (2009b) "Identifying the Regional Economic Impacts of 9/11," *Peace Economics, Peace Science and Public Policy*: Vol. 15 : Iss. 2, Article 6.

Park, JY and P Gordon, 2005, “An Evaluation of Input-Output Aggregation Error Using a New MRIO Model” Paper presented at *North American Meetings of the Regional Science Association International 52nd Annual Conference*, Riviera Hotel & Casino, Las Vegas, NV, November 10-12

Park, JY, 2012, “Application of a Price-Sensitive Supply-Side Input-Output Model to an Examination of the Economic Impacts of Hurricane Katrina and Rita Disruptions of the US Oil-Industry,” *Ecological Economics* (accepted)

Park, JY, J Cho, and A Rose, 2011, “Modeling a Major Source of Economic Resilience to Disasters: Recapturing Lost Production,” *Natural Hazards,* 58 (1): 163-182.

Park, JY, P Gordon, J E Moore II, and H W Richardson, 2009a, “A Two-Step Approach to Estimating State-by-State Commodity Trade Flows,” *The Annals of Regional Science,* 43 (4): 1033-1072.

Park, JY, P Gordon, J E Moore II, and H W Richardson, 2012, “The Interregional and Interindustry Impacts of the Gulf Oil Spill: Applying the National Interstate Economic Model (NIEMO),” *Journal of Homeland Security and Emergency Management* (*forthcoming*)

Perrow, C. 2006. Shrink the targets continued. *Spectrum* 43(9) 46–49.

Polenske, 1980, The US Multiregional Input-Output Accounts and Model, DC Health, Lexington, MA

Poole, R. W., 2007, Airport security: time for a new model. in H.W. Richardson, P. Gordon and J.E. Moore II, eds. *The Economic Costs and Consequences of Terrorism*: 67-97. Cheltenham: Edward Elgar.

Richardson, H. W., P. Gordon, J. E. Moore, II, S.J. Kim, J.Y. Park, and Q. Pan. 2007a. Tourism and Terrorism: The National and Interregional Economic Impacts of Attacks on Major U.S. Theme Parks. in H.W. Richardson, P. Gordon and J.E. Moore II, eds. *The Economic Costs and Consequences of Terrorism*: 235-253. Cheltenham: Edward Elgar.

Richardson, H.W., P. Gordon and J.E. Moore II, eds. , 2007b, *The Economic Costs and Consequences of Terrorism*, Cheltenham: Edward Elgar.

Rose, A, 2004, Defining and measuring economic resilience to disasters, *Disaster Prevention and Management* 13(4): 307-314.

Rose, A. 2007. “Economic Resilience to Disasters: Multidisciplinary Origins and Contextual Dimensions,” *Environmental Hazards: Human and Social Dimensions*, forthcoming.

Rose, A. and D. Lim, 2002, Business interruption losses from natural hazards: conceptual and methodological issues in the case of the Northridge earthquake, *Global Environmental Change Part B: Environmental Hazard*s 4(1): 1-14.

Rose, A., G. Oladosu, and S. Liao. 2007. "Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout," *Risk Analysis*, (27(3): 513-31.

Rose, A.; G. Oladosu; B. Lee; and G.B. Asay (2009) "The Economic Impacts of the September 11 Terrorist Attacks: A Computable General Equilibrium Analysis," *Peace Economics, Peace Science and Public Policy*: Vol. 15 : Iss. 2, Article 4.

Sandler, T. and D. G. Arce M., 2003. "Pure Public Goods versus Commons: Benefit-Cost Duality," *Land Economics*, University of Wisconsin Press, 79(3): 355-368.

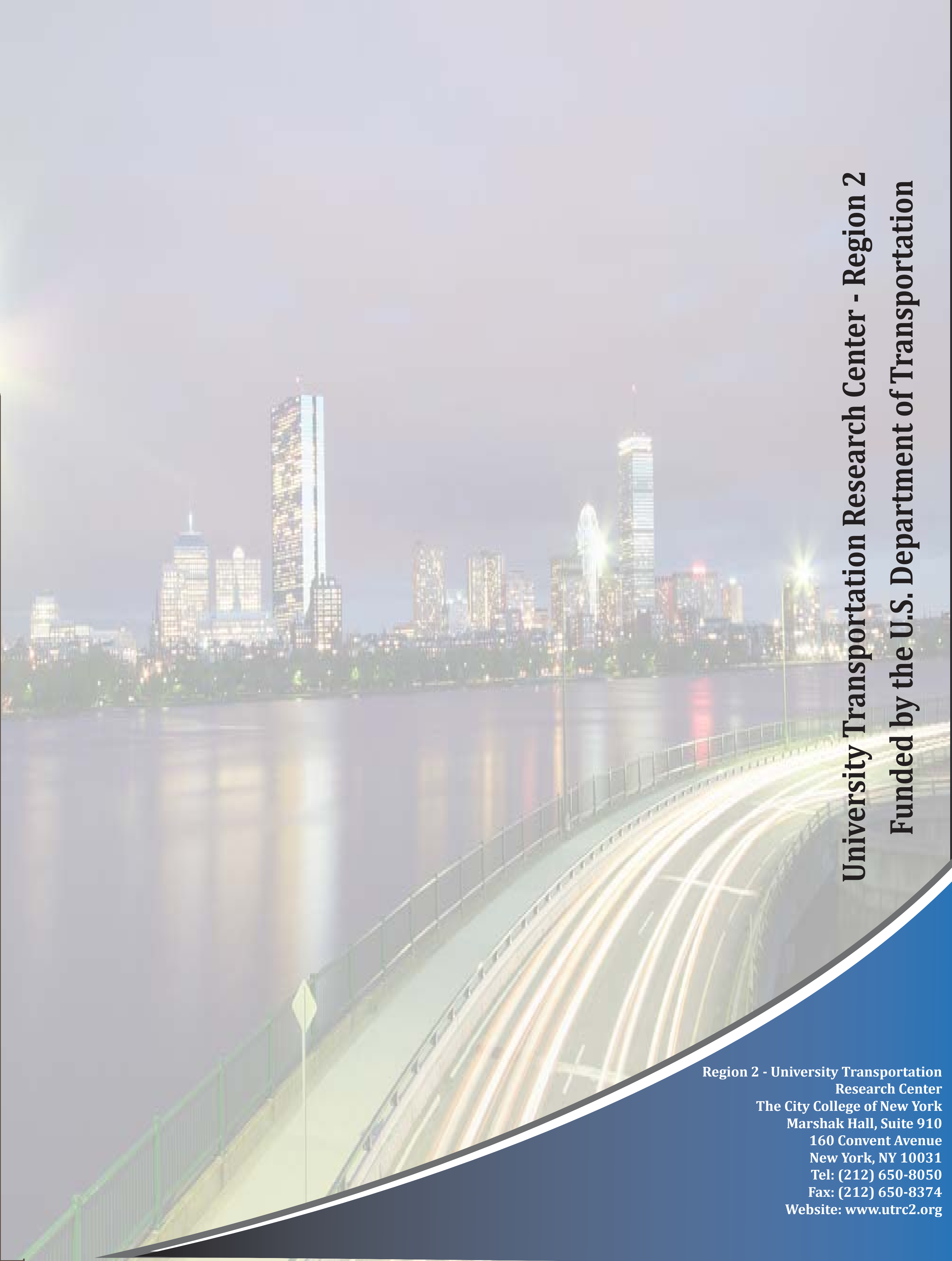
Skaperdas, S. 1996. Contest success functions. *Econom. Theory* 7(2) 283–290.

Tafoya, W. L., 2011, Cyber Terror, *FBI Law Enforcement Bulletin*, November. available at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror (accessed December 2012)

Tirman, J., 2006. Immigration and Insecurity: Post-9/11 Fear in the United States, MIT Center for International Studies. available at http://borderbattles.ssrc.org/Tirman/ (accessed September 2008)

Voice of America News, 2009, Central Bank Says Bangkok Airport Closure Cost Economy $8 Billion, January 12,

Zhuang, J. and V. Bier. Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort, *Operations Research* 55(5) 976–991.



University Transportation Research Center - Region 2
Funded by the U.S. Department of Transportation

Region 2 - University Transportation Research Center
The City College of New York
Marshak Hall, Suite 910
160 Convent Avenue
New York, NY 10031
Tel: (212) 650-8050
Fax: (212) 650-8374
Website: www.utrc2.org