# THE FUTURE OF MANAGING TERRORISM RISK: INDUSTRY CHALLENGES & OPPORTUNITIES

by

Eric W. Vickers

Honors Thesis

Appalachian State University

Submitted to the Department of Finance, Banking, and Insurance

and The Honors College

in partial fulfillment of the requirements for the degree of

Bachelor of Science in Business Administration

May, 2015 of graduation

Approved by:

_____

Dave Wood, Ph.D., Thesis Director

_____

Sandy Vannoy, Ph.D., Second Reader

_____

Sandy Vannoy, Ph.D., Walker College of Business Honors Director

_____

Leslie Sargent Jones, Ph.D., Director, The Honors College

TABLE OF CONTENTS

Abstract

This paper is an examination of the threat of global terrorism and the associated challenges and opportunities in determining the most viable risk management solutions. Terrorism risk poses unprecedented challenges - conceptual, technical, and operational - for the insurance industry. The effects of terrorist events can be enduring, incurring virtually limitless costs and consequences to the economy. Through analysis of the nature of terrorism risk, issues with insurability become apparent. Despite offering coverage for such events, insurers face difficulties in measuring and quantifying terrorism risk to underwrite it profitably. With the current political environment, the uncertainty of the government's role is a concern for insurers, risk managers, and lawmakers. The future of managing terrorism risk is reliant on the industry adopting a solution that is not only feasible in implementation, but also economically sustainable.

## I. Introduction to Terrorism Risk

### a. Terrorism Risk Management

The risk management process is used to minimize the adverse effects of loss exposures and involves the sequence of five steps: 1) identifying and analyzing exposures to loss, 2) examining feasible alternative risk management techniques to handle exposures, 3) selecting the most appropriate risk management techniques to handle exposures, 4) implementing the chosen techniques, and 5) monitoring the results ("Risk Management Process"). Corporations and other organizations use this systematic approach of managing risk to ensure proper measures are being used to lower the total cost of risk. From an industry perspective, the risk management process is essential in understanding the challenges that the government and insurers face as well as opportunities regarding alternative risk transfer methods and financing techniques.

The insurance industry faces significant challenges with terrorism risk in three areas: conceptual, technical, and operational. Conceptual challenges include identification and analysis, technical challenges include quantification and assessment, and operational challenges relate to monitoring the results of the implemented risk management techniques. An in-depth analysis of these challenges can help identify if the current techniques in place are appropriate and if changes should be implemented. A conceptual understanding of terrorism risk and the inherent loss exposures is necessary. Although there may be numerous definitions of terrorism, the Federal Bureau of Investigation defines it as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives" (What We Investigate, 2010). While it is the duty of the government to mitigate terrorist

threats, insurers must be able to understand the risk to be able to effectively analyze the loss exposures and underwrite the risk profitably.

b. Economic Impact

Terrorism risk and its impact on the global economy must be understood to identify the true costs. The macroeconomic effects of such disasters can be immense and have both direct and indirect economic costs. Direct costs are often shorter in nature while the indirect costs can have a greater impact for years to come. Acts of terrorism can have severe economic consequences "by diverting foreign direct investment, destroying infrastructure, redirecting public investment funds to security, or limiting trade" (Sandler and Enders, 2004). The substantive consequences require the industry to respond in a manner that reduces the overall impact to the economy.

Direct impacts including fatalities, injuries, damage to property, and losses to infrastructures can result in immediate disruptions to the economy. Businesses are often unable to adapt to these changing circumstances and recover to pre-loss conditions. Using real-time forecasting, a study looking at certain variables in relation to the events of September 11, 2001, found that, "the immediate impact was to reduce real GDP growth in 2001 by 0.5%, and to increase the unemployment rate by 0.11% (reduce employment by 598,000 jobs)" (Roberts, 2009).

Terrorism also affects the economy in four ways: "1) it adversely affects the capital stock (i.e. human and physical) of the country, 2) terrorist threat induces higher levels of uncertainty, 3) it promotes increases in counter-terrorism expenditures, drawing resources from productive sectors for use in security, and 4) it is known to affect negatively specific

industries such as aviation, insurance, tourism, etc." (Srujan). In addition to the direct losses from terrorist events, levels of uncertainty can have a significant impact on financial markets, commodities, and currencies. With the allocation of resources by the government to thwart terrorist attacks, issues can arise; funds that would have been used to improve the overall economy are then being used for counter-terrorism operations. Additionally, sectors including cruise lines, entertainment, automobiles, and restaurants can all be impacted with a reduction in consumer spending. Due to the presence and sheer impact of terrorist events on the global economy, methods to address the risk at hand must be considered in full to determine the most viable solutions the industry can reasonably implement and maintain.

c. Industry Response

The magnitude of terrorism risk's impact became a reality on September 11, 2001. This pivotal point in history altered the perception of terrorism and changed the way in which it is assessed, evaluated, and treated with respect to insurance mechanisms. Created in response to this event, "the Terrorism Risk Insurance Act (TRIA) filled a critical financial void at a time of great national uncertainty and helped ensure an orderly financial recovery in the event of future events" ("TRIA Backgrounder", 2013). Essentially, TRIA required all property and casualty insurers to provide terrorism coverage for commercial policyholders. In return, the federal government would act as a reinsurer, agreeing to reimburse carriers for losses up to a hard cap of $100 billion.

The stated purpose of TRIA is as follows:

"*To establish a temporary Federal program that provides for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism, in order to-*

*1. protect consumers by addressing market disruptions and ensure the continued widespread availability and affordability of property and casualty insurance for terrorism risk; and*

*2. allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses, while preserving State insurance regulation and consumer protections"* (Roberts, 2004).

This fundamental purpose of TRIA has created additional challenges for insurers despite its intentions to act as a federal backstop and provide a safety net to prevent insurers from becoming insolvent after a catastrophic terrorist event.

One constraint through the creation of TRIA is the role of government intervention and restrictions to take over the market. Various standpoints can be used in determining how to properly address the risk, depending on a corporation's structure. However, the first step is to understand the stipulations inherent to TRIA, including thresholds and other requirements. For example, insurer deductibles are set at twenty percent of premiums – the amount that must be paid before federal assistance is provided. Additionally, there are certain requirements that must be met in order for coverage to apply with regards to certified acts of terrorism.

"Only certified acts are eligible for coverage through TRIA. An event can be certified if the Secretary of the Treasury, the Secretary of State, and the Attorney General of the United States determine the act meets all the following criteria:

- It is considered an act of terrorism.
- It is violent or dangerous to human life, property, or infrastructure.
- It results in damage within the United States, (including US air carriers, vessels, and/or US missions, as described in the Act).
- It is committed by an individual or individuals, as part of an effort to coerce the US civilian population or to influence the policy or affect the conduct of the US government by coercion." ("Certifying Events Under").

Having been recently extended to 2020, the Terrorism Risk & Insurance Program Reauthorization Act of 2007 provides a level of security to the insurance industry. However, much debate has occurred questioning if this will serve as a temporary fix or a permanent solution to the problem. Given TRIPRA's stipulations, insurers must understand how to properly identify, analyze, and measure the risk. While this and other issues create challenges for insurers in the underwriting process, opportunities for the private sector may exist in the future, depending on the industry's direction.

## II. Insurer Challenges

a. Hazard Identification

The first phase in the risk management process poses additional challenges to insurers and the government to identify and analyze the threat of terrorist organizations. Understanding where terrorism risk exists and the hazards involved are essential to

understand prior to beginning the quantification and assessment stages. "Terrorism risk only exists when a person or group has the *capability* and *intent* to present a *threat* of attack on a *vulnerable* target in a manner which would have *consequences* of concern to citizens of the United States" (Willis, 2008). When utilizing hazard identification, insurers must use an approach that encompasses an in-depth look at historical occurrences, current threats, and emerging threats. Additionally, understanding terrorist organizations in light of the true threat level is crucial. Lastly, it is critical that the influence of risk perception is not substantial enough that it alters the true impact of terrorist threats in the following steps to measure and quantify the risk.

Historical terrorist events can provide insight into the frequency of such occurrences as well as the severity of losses. Terrorist events have been extremely costly over the years, with millions in property damage and many fatalities. The following chart illustrates the impact that past events have had:

| Date | Country | Event | Insured Property Loss (USD Million)* | Fatalities |
|---|---|---|---|---|
| September 11, 2001 | United States | Attacks in New York and Washington DC | 23,870 | 2,982 |
| April 24, 1993 | United Kingdom | IRA bomb attack in London | 1,152 | 1 |
| June 15, 1996 | United Kingdom | IRA bomb attack in Manchester | 946 | 0 |
| April 10, 1992 | United Kingdom | IRA bomb attack in London | 852 | 3 |
| February 26, 1993 | United States | World Trade Center bomb attack | 794 | 6 |
| July 24, 2001 | Sri Lanka | Tamil Tiger attack at Colombo Airport | 507 | 20 |
| February 9, 1996 | United Kingdom | IRA bomb attack in London | 329 | 2 |
| April 19, 1995 | United States | Oklahoma City bomb attack | 185 | 166 |
| April 11, 1992 | United Kingdom | IRA bomb attack in London | 122 | 0 |
| November 26, 2008 | India | Attacks and shootings in Mumbai | 107 | 172 |

SOURCE: INSURANCE INFORMATION INSTITUTE, SWISS RE, U.S. BUREAU OF LABOR STATISTICS *All losses adjusted to 2011 dollars

Over the past few decades, the terrorism landscape has evolved in a number of ways. With growing threats from organizations such as Al-Qaeda and Al-Shabab, global terrorism

risk is imminent. RAND, a world leader in research on terrorism, published a study stating, "terrorism remains a real-albeit uncertain-national security threat, with the most likely scenarios involving arson or explosives being used to damage property or conventional explosives or firearms used to kill and injure civilians" (Hartwig and Wilkinson, 2014). Terrorist organizations will often use threats in an attempt to create fear among the public through use of weapons of mass destruction, including incendiary, chemical, biological, radiological, and nuclear agents. Additionally, hazards can vary greatly from conventional bombs, armed attacks, and assaults on infrastructures and information systems.

While common terrorist hazards must be identified, it is even more crucial to identify new and emerging trends. One such trend that is perhaps the biggest threat in the real of terrorism is cyber-terrorism. The Central Intelligence Agency has identified this threat as the battleground for the future regarding terrorist hazards. James Clapper, U.S. Director of National Intelligence, recently stated in a hearing that cyber attacks, allegedly by North Korean and Iranian groups, "against us are increasing in frequency, scale, sophistication and severity of impact" (Paletta, 2015). These highly targeted events use Internet attacks in the attempt to disrupt networks on a large-scale. Cyber-terrorism and other emerging trends must be identified for insurers to begin the analysis process.

The role of social media and other similar technological platforms must be identified as an emerging threat with terrorist organizations. With the ubiquitous nature of social media, extremists have the ability to recruit new members and exchange information much more rapidly than ever before. Governments must use resources to identify threats, monitoring areas of political turmoil and assessing the hazards that may be involved in possible terrorist events ("Tensions Building," 2012).

Regarding risk perception, insurers and governments must be careful to separate the concept of risk with hazard identification. "The concept of risk is a psychological one. Risk, as opposed to danger, is a socially constructed phenomenon. Riskiness is based on perception rather than fact, and this perception is based on qualitative, not qualitative characteristics of the hazard being considered" (Jenkin, 2006). While there are attributes to risk such as probability and voluntariness, it is important to understand that no single attribute defines the risk of a particular hazard. This being said, the influence of risk perception, especially with regards to political or terrorism risk, should be taken into consideration when identifying the threats of hazards in the identification process. By doing so, governments and insurers will be better prepared to fully assess the likelihood of terrorist threats without placing a significant emphasis on risk perception.

b. Analysis

Through the analysis stage, terrorism risk can be viewed to identify the key determinants in properly assessing the risk as well as looking at the issue of insurability. The three primary determinants in assessing terrorism risk include: 1) threat, 2) vulnerability, and 3) consequences. "Terrorism risk indicates the expected consequences of attacks considering the possibility of the occurrence and success of the terrorist attacks. In terms of probability, a terrorism risk from an attack of a certain type is the unconditional expected value of damages of a certain type" (Srujan). While this may seem like a simple process, the reality of understanding this risk in full is a difficult task.

Despite the requirements for insurers to provide coverage for terrorism, an analysis to determine insurability can be made to understand if the current system is economically

sustainable. Alfred Manes described insurance as follows: "insurance is the mutual cover of a fortuitous, assessable need of a large number of similarly exposed businesses" (Thomas, 2005). Not only is this necessary in understanding the nature of the risk itself, but also in understanding the options available as it pertains to the quantification of the risk.

Certain conditions should be true in order for insurance to work as a method of risk sharing. To determine insurability of a risk, there are four basic requirements: 1) estimable frequency, 2) estimable severity, 3) diversifiable risk, and 4) random loss distribution (Colodny, Fass, Talenfeld, Karlinsky, Abate, and Webb, 2013). Terrorism risk can be classified as systemic in nature because it is non-diversifiable, difficult to predict, and impossible to completely avoid. This violation of the technical definition of an "insurable" risk creates many challenges for insurers. Since there are very few data points regarding the frequency with which terrorist attacks occur, it is nearly impossible to use models to estimate their likelihood with any actuarial credibility. Additionally, it is difficult to model the possible losses an insurer could sustain due to the magnitude of losses. Terrorism risk is likely to be highly concentrated in a geographic area, within an industry, or within a certain time span. Finally, insurability requires losses to be random or fortuitous. Terrorism events are planned and coordinated events, violating the need for randomness in nature.

A comparison to catastrophic risks such as natural disasters has been made, but there are several key differences and factors which include: "availability of historical data, dynamic uncertainty, shifting attention to unprotected targets, existence of negative externalities and government influencing the risk" (Kunreuther and Michel-Kerjan, 2004). The first difference is a primary issue in the quantification phase of the risk management process in that there is a severe lack of historical data available for use, primarily due to

national security reasons. One way in which terrorism is analyzed is through rates. However, issues arise in that base rates for terrorist losses are significantly lower than those related to, for example, homicide or deaths as a result of cardiovascular disease. Assessing other risks for insurance purposes are less difficult due to this and other reasons.

Dynamic uncertainty involves the issues of a combination or mix of strategies and counterstrategies used in a terrorist attack. These are very difficult to accurately analyze. Through these strategies, terrorists will often respond to security measures by shifting their attention to more vulnerable targets. Negative externalities such as information sharing and interdependent security are also factors. Perhaps the most differentiating factor is the role that government has in attempts to mitigate threats and thwart potential disasters. All of these factors must be included in the analysis and pose issues from an insurability standpoint.

Before beginning the modeling process, insurers must understand the government's initiatives to prevent terrorist attacks. This can pose issues in the quantification and measurement of terrorism risk. While an approach can be made similar to that used in catastrophe modeling, the quantification of counter-terrorism operations are nearly impossible. In addition to the coverage provided under TRIA's enactment through the partnership of private insurers and the government, methods exist through loss control and preventative measures. The government has the duty to identify, analyze, measure, and treat the risk of terrorism to protect the nation as a whole. The primary way in which the government treats terrorism risk is through proactive measures. One of the challenges that the government faces is finding the balance between counter-terrorism attempts and emergency management. Governments must take policy measures to prevent terrorism, but they should resist contributing to institutionalized fear. Governments should prepare policy

measures for mitigation, preparedness, response, and recovery for these hazards. While these operations are essential, insurers have difficulties in incorporating these measures into the modeling process.

While it is difficult to approach terrorism risk in a way that identifies the frequency and severity of terrorist events, the U.S. Department of Homeland Security (DHS) attempts to identify and analyze the risk through a qualitative approach. In the absence of sound risk assessment methods, the prioritization of homeland security activities at the federal, state, and local level is problematic. DHS's primary mission is to assess risk in an accurate manner, analyzing the threats that exist. Utilizing a color-coded warning system, DHS classifies the current threat level at any given time. Similar to a risk map used in the risk management process, this warning system analyzes the current intensity levels, indicating which governmental actions need to be taken. Threat levels are classified as: 1) severe, 2) high, 3) elevated, 4) guarded, and 5) low. This method is particularly useful for understanding, analyzing, and assessing the current threat level that the United States faces. Additionally, this method highlights the differing nature of terrorism from other catastrophic risks, considering the plans and procedures in place for governmental intervention. Regardless of the viewpoint on terrorism, the government and insurers have challenges in appropriately assessing the risk and using a risk management approach in the allocation of resources to treat the exposures.

c. Quantification Methods

From a technical standpoint, insurers face challenges when quantifying and measuring terrorism risk to model it appropriately. The risk landscape resulting from the

events of September 11th radically changed and created problems for insurers in the risk assessment process. However, the first and most important step is understanding the insurer's role in this process. "For terrorism as with natural hazards, a catastrophe risk analyst's task is to assess the likelihood of an event occurring, not to predict, let alone prevent, an event" ("Quantifying U.S. Terrorism Risk"). Insurers must use methods to evaluate the risk being insured, subject to constraints in this process.

Through analysis, we understand the problems that insurers face. "The events of 11 September have shown that people, rather than nature, pose the biggest risks, and that it is necessary to consider the maximum *imaginable* loss, not just the maximum possible loss" (Stahel, 2003). In considering the extent of these losses, risk modeling can be used to assess the risk for rating purposes. "RMS' industry-leading terrorism model simulates over 90,000 large-scale terrorist attacks across 9,800 global targets using 35 different attack types" ("Quantifying U.S. Terrorism Risk"). Models such as this are not, however, perfect by any means. In fact, there are several issues inherent to these models due to the nature of terrorism risk.

In addition to the issues stated previously, other issues include: 1) the inability to model human behavior, 2) the restricted access to classified information, and 3) pricing with precision and accuracy. The first issue is based on the premise that it is virtually impossible to model human behavior. In economic models such as RMS, the assumption is made that terrorists will seek to maximize loss subject to security constraints. In theory, this approach views terrorists in a way that determines that they will make a rational decision. Psychologically speaking, terrorists are not logical and rational beings. Rather, they are unpredictable and difficult to understand. Attempting to predict and model behavior is not

only inefficient, but it is also unnecessary. Government officials, at a tactical level, should be responsible for dealing with this threat.

Another issue involves the inability to access classified information. This issue greatly restricts insurers' ability to assess the likelihood of terrorist attacks. Classified information and other highly sensitive data are not available to predict the next terrorist event. While insurers attempt to assess the likelihood of these events occurring, it is the government's duty to predict the next events. In this role, the government engages in counter-terrorism attempts. With regards to quantifying terrorism risk in a matter that incorporates the government's counter-terrorism operations, game theory analysis can be used. In its most simple form, game theory analysis looks at the uncertainty in the decision-making process, identifying the possibilities in conflict situations. This is particularly important with terrorism risk due to the nature of terrorists seeking to maximize loss, subject to security constraints. "Current application of methods of Game Theory in study of terrorism include: evaluation of strategy how nations allocate funds to combat terrorism and how they deal with situations after the attack, assessment of risks associated with terrorism, determines whether state policy of not negotiating with terrorists discourage these activities" (Fuka, Obrsalova, and Langasek, 2012). While the government can benefit from analyzing game theory tactics and responding in the most appropriate manner, insurers are unable to incorporate this and other classified information as underwriting data.

d. Rating & Evaluation

The inability to accurately model terrorism risk creates challenges for evaluating the financial solvency of insurance carriers that underwrite this risk. As previously stated,

insurers are required to offer this coverage and should then be assessed by rating agencies to evaluate the financial strength. A.M. Best released a report stating the challenges in their assessment of this issue. Insurers' risk profiles are assessed through stress tests, looking at the impact of losses on their financial statements and overall solvency levels. Various approaches are used depending on the aspect with which the insurer is assessed. For example, reinsurers and primary insurers must be assessed in a way that accurately projects the overall risk level. Additionally, differences due to the trigger of TRIA's federal backstop alters the evaluation of carriers (Draft: The Treatment of Terrorism Risk in the Rating Evaluation, 2015). Overall, the level of detail needed to truly assess insurer's financial strength is limited to the scope with which terrorism risk can be modeled and evaluated.

In evaluating insurers for solvency standards and other metrics, issues become apparent with the imposition of requirements. In the London market, syndicates share a proportional amount of exposure to loss. Lloyd's is one of the primary markets to insure complex risks, and terrorism is often covered here. To ensure the impact of terrorist events will be spread amongst syndicates as to not disrupt the market, Lloyd's maintains a set of mandatory Realistic Disaster Scenarios (RDS) to stress test both individual syndicates and the market as a whole ("RMS Terrorism Solutions"). The event scenarios are regularly reviewed to ensure they represent material catastrophe risks. One of the primary measures that RDS looks at is exposure accumulation. "One problem insurers face is the accumulation of risk. They need to know not only the likelihood and extent of damage to a particular building but also the company's accumulated risk from insuring multiple buildings within a given geographical area, including the implications of fire following a terrorist attack" ("Terrorism Risk & Insurance"). Blast zone radiuses are mapped by insured locations to

determine what the aggregate exposure of any one syndicate is. While this may be useful, there are inherent issues. The measurement is superficial because it only takes exposure accumulation into effect. Until regulation changes, syndicates and the London market will continue to be assessed using this and other measures.

## III. The Future of the Industry

### a. Public Policy Approaches

The future of managing terrorism risk is still uncertain, especially regarding the government's role. Concernign market failures in the insurance industry, there are essentially three approaches to public policy: 1) laissez-fare policy, 2) public interest theory, and 3) market-enhancing view. Laissez-faire public policy views limited government intervention as optimal due to the belief that a market-based equilibrium will provide the most efficient allocation of resources. Oppositely, the public interest theory of regulation suggests that, in the existence of market failures, the government can and will provide solutions for the overall economy. Proponents of this theory suggest that the government should, essentially, complete the terrorism insurance market. Lastly, the market-enhancing view takes a position between the other two approaches. In this view, the belief is that public policy should facilitate the development of the private market, such as by improving information flows, but should not create new federal institutions to substitute for private solutions (Brown, Cummins, Lewis, and Wei, 2004). Despite differing opinions on this matter, the most optimal approach will be dependent on changing legislation and the existence of market failures, monitoring the implemented risk management techniques to determine if changes need to be implemented.

b. Opportunities

From an operational standpoint, the insurance industry faces numerous challenges in the treatment of terrorism risk. The future of managing terrorism risk is hinged on uncertainty, raising concerns regarding the current model in place to handle terrorist events. Principally, there are two options that exist with regard to providing solutions to this ever-changing problem. The first involves the continued model through government intervention, providing a federal backstop to the industry. Secondly, insurers with interest in insuring terrorism risk can move towards a privatized industry. The question remains on what constitutes the most viable option that can be easily implemented and is inherently sustainable from an economic stance. Regardless of which solution will be used in the future, the government and insurers must collaborate to minimize effects of threats and capture the opportunities.

The first solution is perhaps the most viable in scope due to the smaller changes that need to take place for implementation. The subsidized insurer model through public-private partnerships that is currently in place is necessary due to the government's involvement in terrorism risk. Changes can, however, be implemented that will provide for a more stable environment with which to handle terrorism risk. Since the government is unable to release classified information, one solution could be the inclusion of this information solely for the purposes of modeling efforts. For example, private insurers use public and historical data to assess the likelihood of a loss but need additional data to finish the model. The government could act by establishing its own modeling tool using classified data to assist private insurers in more accurately rating and pricing the risk being insured. This is an interest for both

parties if the government continues to act as a federal backstop to insuring losses of terrorist acts, subject to certain requirements.

The second solution to the problem is the privatization of the industry and eliminating or reducing the government's role in terrorism risk. If there is a realistic possibility for insurance carriers to underwrite terrorism risk profitably, this would be the idealistic situation. The E & S industry typically underwrites unique risks without much historical data, capturing the opportunities that the admitted market is not able to or willing to take. Additionally, insurers in this market enjoy the freedom of rate and form, not being restricted by ISO forms or pricing techniques. However, as previously discussed, there are certain barriers that exist which prevent carriers to model terrorism risk. Although this possibility remains, it is difficult to understand how this would be accomplished given the issues and the unique nature of terrorism.

With respect to private markets, companies have various constraints in insuring terrorism risk. For example, companies have a finite amount of capital and reserves and, in order to maintain sufficient capital for CAT losses, costs can be substantial due to tax and accounting constraints. However, according to Jaffee and Russell, "with respect to the insurability of catastrophe risk, when these risks are free to be priced to yield a reasonable profit, and assuming that creative financial engineers can find ways to raise the capital necessary to fund losses, there is no obvious reason why private insurance markets should not be able to provide this product" (Jaffee, 2005). This is why there is tremendous opportunity in the E & S industry to handle this risk.

In addition to these opportunities, there may be potential in the capital markets. However, there are several factors preventing financial instruments such as terrorism bonds

from having a share of the risk (Woo). Much of the concern with terrorism risk insurance is similar, but there are three main reasons why investors will not invest in terrorism bonds. The reasons include, 1) the correlation between terrorism and equity markets, 2) greater potential for adverse selection, and 3) reluctance of rating agencies to rate these bonds (Sclafane, 2013). Financial markets are highly sensitive to terrorist events and investors are unwilling to take this risk because the return needed to justify the cost is unlikely to be profitable. In addition, those seeking terrorism bonds would likely be the ones who need it the most, alluding to the issue of adverse selection. While rating agencies have been unwilling to look at rating terrorism bonds, Standard & Poor's released a report last year stating that it is open to rating new risks that could be covered using insurance-linked securities. "If some method could be devised to sensibly structure cat bond or ILS type instruments to transfer the risks of property damages from terror attacks to the capital markets as well, we could get some way towards a privately supported terrorism reinsurance backstop" (ILS Forum, 2014).

For the market to become fully privatized and functional in underwriting, necessary changes would need to occur that are not likely to happen. Information sharing between governmental agencies and insurance underwriters would need to take place to begin modeling terrorism risk more accurately, considering external factors such as counter-terrorism operations and classified information. Recently, the government announced the establishment of the Cyber Threat Intelligence Integration Center in an effort to assist businesses with cyber crime. Shortly thereafter, "the Cyber Threat Sharing Act of 2015, S. 456, which is aimed at removing barriers in order to increase the sharing of cyber threat data between private industry and the federal government," was enacted (U.S. Needs to Construct

National Cyber Security Policy, 2015). This provides insight into the future of managing terrorism risk if such initiatives take place to increase the sharing of data between the government and private insurers. This will greatly increase insurers' ability to understand terrorism risk and model it accordingly, considering externalities such as counter-terrorism operations.

## IV. Conclusion

The insurance industry as a whole must address the issues inherent in managing terrorism risk, opting for solutions that are economically sustainable for the future. "Questions remain as to whether the private markets have developed to the point of offering terrorism insurance to all willing to purchase it; whether the cost of such coverage would be affordable; and, whether the private insurance industry would have sufficient capital available to withstand the potentially most catastrophic terrorist attacks" (Roberts, 2009). The private market for terrorism insurance, especially the E & S industry, has great potential to profitably underwrite this risk, eliminating the need for the government acting as the "insurer of last resort." "On the other hand, even if private insurers and reinsurers develop instruments to cope with a $100b loss, it is unreasonable to suppose that the loss itself will not be disruptive" (Jaffee and Russell, 2005). Despite insurability issues inherent with terrorism risk, opportunities exist in the private markets. If the government is willing and able to provide insight into its counter-terrorism operations, there may be a possibility for the industry to become fully privatized.

Regardless of the model used in managing terrorism risk, collaboration will be needed for insurers to assess the likelihood of an event in conjunction with the government

using mitigation strategies to thwart potential attacks. As stated before, there is much debate over the three theories of economic public policy regarding the most optimal approach. However, the government can and should support the private market for terrorism insurance without placing unnecessary restrictions that would otherwise create additional challenges in the pursuit of managing this incredibly complex risk.

## V. Bibliography

Brown, J., Cummins, D., Lewis, C., & Wei, R. (2004, April 29). An empirical analysis of the economic impact of federal terrorism reinsurance. Retrieved February 8, 2015, from http://business.illinois.edu/jbrown/Mypapers/JME%20TRIA.pdf

Colodny, Fass, Talenfeld, Karlinsky, Abate, & Webb. (2013, September 26). U.S. Senate Committee Considers TRIA Reauthorization. Retrieved February 16, 2015, from http://www.wci360.com/news/article/u.s.-senate-committee-considers-tria-reauthorization

Fuka, J., Obrsalova, I., & Langasek, P. (2012, October 13). Game Theory Application on Terrorism. Retrieved from February 10, 2015, from http://www.wseas.us/e-library/conferences/2012/Zlin/EPRI/EPRI-37.pdf

Hartwig, R., & Wilkinson, C. (2014, March 1). Terrorism Risk: A Constant Threat. Retrieved February 16, 2015, from http://www.iii.org/sites/default/files/docs/pdf/terrorism_white_paper_0320141_0.pdf

Jaffee, D., & Russell, T. (2005, August 1). Should Governments Support the Private Terrorism Insurance Market? Retrieved February 8, 2015, from http://www.scu.edu/business/faculty/research/upload/wp06-09-russell-terror-insurance.pdf

Jenkin, C. (2006, July 1). Risk Perception and Terrorism: Applying the Psychometric Paradigm. Retrieved February 10, 2015, from https://www.hsaj.org/articles/169

Kunreuther, H., & Michel-Kerjan, E. (2004, March 25). Insurability of (Mega)-Terrorism Risk: Challenges and Perspectives. Retrieved February 10, 2015, from http://mason.gmu.edu/~rhanson/PAM/PRESS2/OECD-3-04.pdf

Roberts, B. (2009, August 1). The Macroeconomic Impacts of the 9/11 Attack: Evidence from Real-Time Forecasting. Retrieved February 16, 2015, from https://www.dhs.gov/xlibrary/assets/statistics/publications/ois_wp_impacts_911.pdf

Roberts, D. (2004, November 16). Terrorism Risk Insurance: Conceptual Issues. Retrieved February 10, 2015, from http://www.coffi.org/pubs/TRIAprimerp2.pd

Roberts, K., & Horgan, J. (2008, November 6). Risk Assessment and the Terrorist | Roberts | Perspectives on Terrorism. Retrieved February 10, 2015, from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/38/html

Sandler, T., & Enders, W. (2004, January 1). Economic Consequences of Terrorism in Developed and Developing Countries: An Overview. Retrieved February 16, 2015, from http://www.utdallas.edu/~tms063000/website/Econ_Consequences_ms.pdf

Sclafane, S. (2013, September 19). Terror Risk Bond Market Unlikely, Says Swiss Re Americas CEO - Carrier Management. Retrieved February 16, 2015, from http://www.carriermanagement.com/news/2013/09/19/113254.htm

Srujan, A. (n.d.). Issues in Terrorism Risk Management. Retrieved April 14, 2015, from http://www.actuariesindia.org/downloads/gcadata/10thGCA/Issues in Terrorism Risk Management_A Srujan.pdf

Stahel, W. (2003, July 1). The Role of Insurability and Insurance. Retrieved February 16, 2015, from https://www.genevaassociation.org/media/240594/ga2003_gp28(3)_stahel.pdf

Thomas, B. (2005, October 1). Terrorism – Exposures, Insurability, Pools and Other Solutions. Retrieved April 14, 2015, from http://actuaries.asn.au/Library/gipaper_thomas0510.pdf

Willis, H. (2008, June 1). Challenges of Applying Risk Management to Terrorism Security Policy. Retrieved February 24, 2015, from http://www.rand.org/content/dam/rand/pubs/testimonies/2008/RAND_CT310.pdf

Woo, G. (2002, February 1). QUANTIFYING INSURANCE TERRORISM RISK. Retrieved February 10, 2015, from http://www.rit.edu/~w-cmmc/literature/Woo_2002b.pdf

Woo, G. (n.d.). QUANTITATIVE TERRORISM RISK ASSESSMENT. Retrieved March 10, 2015, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.1362&rep=rep1&type=pdf

Certifying Events Under the Terrorism Risk Insurance Act. (2013, April 19). Retrieved February 16, 2015, from https://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/30561/Certifying-Events-Under-the-Terrorism-Risk-Insurance-Act.aspx

Draft: The Treatment of Terrorism Risk in the Rating Evaluation. (2015, February 6). Retrieved February 16, 2015, from http://www3.ambest.com/ambv/ratingmethodology/OpenPDF.aspx?rc=233264

ILS Forum Debates Viability of Terrorism Bonds. (2014, December 3). Retrieved February 10, 2015, from http://www.intelligentinsurer.com/news/ils-forum-debates-viability-of-terrorism-bonds-1960

Quantifying U.S. Terrorism Risk. (n.d.). Retrieved February 16, 2015, from http://static.rms.com/email/documents/quantifying_us_terrorism_risk.pdf

Risk Management Process. (n.d.). Retrieved February 10, 2015, from http://www.irmi.com/online/insurance-glossary/terms/r/risk-management-process.aspx

RMS Terrorism Solutions. (n.d.). Retrieved March 10, 2015, from http://riskinc.com/Publications/RMS_Terrorism_Solutions.pdf

Tensions Building: The Changing Nature of Terrorism Risk and Coverage. (2012, December 1). Retrieved February 10, 2015, from http://www.scor.com/en/sgrc/pac/terrorism/item/2084-tensions-building-the-changing-nature-of-terrorism-risk-and-coverage/2084-tensions-building-the-changing-nature-of-terrorism-risk-and-coverage.html

Terrorism Risk and Insurance. (2015, January 1). Retrieved February 10, 2015, from http://www.iii.org/issue-update/terrorism-risk-and-insurance

TRIA Backgrounder. (2013, January 1). Retrieved February 16, 2015, from http://www.aiadc.org/aiapub/content.aspx?id=360668

U.S. Needs to Construct National Cyber Security Policy. (2015, February 15). Retrieved February 16, 2015, from http://www.businessinsurance.com/article/20150215/NEWS06/302159999/u-s-needs-to-construct-national-cyber-security-policy?tags=|302

What We Investigate. (2010, November 5). Retrieved February 16, 2015, from http://www.fbi.gov/albuquerque/about-us/what-we-investigate