Terrorism Risk: Industry Challenges & Opportunities

by

Eric W. Vickers, UACIC

Senior

Appalachian State University

Dr. David Wood, CPCU, CRM

Terrorism Risk: Industry Challenges & Opportunities

I. Introduction

The threat of global terrorism 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.

II. Terrorism Risk – Economic Impact & Industry Response

A conceptual understanding of terrorism and the inherent loss exposures is essential. The Federal Bureau of Investigation defines terrorism 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). 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). Due to the sheer impact of terrorist

events on the global economy, methods to address the risk must be considered in full.

The magnitude of terrorism risk and its 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 $100 billion. The fundamental purpose of TRIA was to create a temporary partnership between the government and private insurers, providing a safety net to prevent insurers from becoming insolvent after a catastrophic terrorist event.

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.

III. Identification of Threats

When utilizing hazard identification, insurers must use an approach that encompasses an in-depth look at historical occurrences, current exposures, and emerging trends. Historical events can provide insight into the frequency of such occurrences as well as the severity of losses. Listed below is a chart depicting the costliest terrorist events in recent years:

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 ISIS, 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 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 realm of terrorism is cyber-terrorism. 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.

IV. Analysis of Insurability

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, "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.

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, terrorism events are planned and coordinated events, not fortuitous.

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). Due to national security reasons, data from terrorist events are nearly impossible to obtain. The second difference is the uncertainty of terrorists' responses with respect to counterstrategies and attention shifting 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.

V. Quantification & Rating Challenges

From a technical standpoint, insurers face challenges when quantifying and measuring terrorism risk. 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. In addition, insurers face difficulties in maintaining adequate surplus to maintain their financial ratings.

"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.

Some of the primary issues with modeling terrorism risk 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. Attempting to predict and model behavior is not only inefficient, but it is also unnecessary.

Another issue involves the inability to access classified information. The government's role in counter-terrorism operations and emergency management plans are not publically available data. Economic game theory applications with respect to terrorism provide a complex framework that could greatly impact insurers in different regions or locations. Additionally, the government's policy measures for mitigation, preparedness, response, and recovery cannot be accessed to incorporate as underwriting criteria. While an approach can be made similar to that used in catastrophe modeling, the quantification of terrorism risk in full is nearly impossible without access to this information.

The inability to accurately model terrorism risk also creates challenges for the rating of insurance carriers. 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. Differences due to the trigger of TRIA's federal backstop also alter 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.

VI. The Future of the Industry

From an operational standpoint, the insurance industry faces numerous challenges in the treatment of terrorism risk. Alternative solutions to the current subsidized insurer model through public-private partnerships exist, primarily in the E & S industry. The question remains on what constitutes the most viable option that can be easily implemented and is sustainable from an economic stance.

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. Although this possibility remains, it is difficult to understand how this would be accomplished given the issues and the unique nature of terrorism.

For the market to become fully privatized and functional in underwriting, necessary changes would need to occur that are unlikely to happen. Information sharing between governmental agencies and insurance underwriters would need to take place to begin modeling terrorism risk more accurately. 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.

VII. Conclusion

The insurance industry must address the issues inherent to managing terrorism risk, opting for solutions that are economically sustainable for the future. 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). 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 privatized. Regardless of the chosen model used to manage terrorism risk, collaboration will be needed for insurers to assess the likelihood of an event in conjunction with the government's mitigation tactics to thwart potential attacks.

Works Cited

Colodny, Fass, Talenfeld, Karlinsky, Abate, & Webb. (2013, September 26). U.S. Senate Committee Considers TRIA Reauthorization. Retrieved February 8, 2015, from http://www.wci360.com/news/article/u.s.-senate-committee-considers-tria-reauthorization

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 12, 2015, from http://www.scu.edu/business/faculty/research/upload/wp06-09-russell-terror-insurance.pdf

Kunreuther, H., & Michel-Kerjan, E. (2004, March 25). Insurability of (Mega)-Terrorism Risk: Challenges and Perspectives. Retrieved February 16, 2015, from http://mason.gmu.edu/~rhanson/PAM/PRESS2/OECD-3-04.pdf

Paletta, D. (2015). U.S. Intelligence Officials Say Global Threats Persist From Russia, Terrorists. *Wall Street Journal*. Retrieved February 27, 2015, from http://www.wsj.com/articles/u-s-intelligence-officials-say-global-threats-persist-from-russia-terrorists-1424974534?tesla=y

Sandler, T., & Enders, W. (2004, January 1). Economic Consequences of Terrorism in Developed and Developing Countries: An Overview. Retrieved February 8, 2015, from http://www.utdallas.edu/~tms063000/website/Econ_Consequences_ms.pdf

Stahel, W. (2003, July 1). The Role of Insurability and Insurance. Retrieved February 12, 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 February 16, 2015, from http://actuaries.asn.au/Library/gipaper_thomas0510.pdf

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

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

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

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

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