The TRIA Cyber Risk Coverage Debate
Should Be Resolved as Part of its Renewal

By

Gregory J. May
Nelson Mullins LLP
Boston, MA

Executive Summary

Lost in the commotion over whether Congress should reauthorize the Terrorism Risk Insurance Act ("TRIA") at all is the question of whether TRIA, as it is written today, does enough to protect the United States from the actual terrorist threats we now face. There is a growing danger posed by cyber terrorist attacks aimed at harming our nation's electronic infrastructure. Government officials and business leaders agree that the next terrorist attack on the United States will most likely be a cyber attack on financial, energy or other business networks designed to significantly disrupt the national economy. The fear is that any such successful attack could wipe out billions of dollars in assets and paralyze financial, energy and telecommunications systems.

Like terrorism insurance, cyber insurance, which is designed specifically to cover businesses from losses arising from attacks on electronic networks and systems, is in its relative infancy. Recent data breaches have spurred many businesses to seek cyber risk coverage. The insurance industry is responding, but industry leaders admit that they do not yet have the expertise to securely underwrite cyber risks. A TRIA backstop extending to losses from cyber attacks would provide more certainty to businesses and insurers who are responsibly seeking to insure against this new and serious cyber threat.

TRIA’s statutory language does not explicitly state that losses resulting from cyber attacks will be covered by the TRIA backstop. Given the magnitude of the cyber threat, TRIA should be amended to confirm that losses resulting from cyber attacks will be covered without any increase in the $100 billion cap provided in the existing TRIA program.

According to Government Agencies and Business Leaders, the Threat of a Catastrophic Cyber Terrorist Attack Is Very High.

Department of Homeland Security ("DHS") officials, law enforcement agency heads, politicians and business leaders have recently warned that cyber attacks pose the most significant and immediate terrorist threat to the United States. While such attacks may not result in bloodshed or the physical destruction of real estate or other property, the economic effects of a well-executed attack on cyber infrastructure could result in catastrophic monetary losses and the crippling of financial, energy and transportation systems.
What is a "cyber attack" and how could it cause harm? Recent highly publicized cyber incidents such as the data breach at Target are considered to be pure theft of customer data to be used by the perpetrators for their own financial gain. The type of terrorist "cyber attack" feared by security agencies and experts is of a different nature and scale. Terrorists intent on harming American economic interests are believed to be planning attacks on networks maintained by financial markets and energy companies. An attack on a major bank's network could destroy financial data and thus wipe out any record of millions of account holders' assets. An attack on an electric utility's network could disable the utility's ability to manage the power grid and thus paralyze large areas of the country.

Security experts believe that the risk/reward analysis will lead terrorists to pursue cyber attacks rather than the use of deadly force. The 9/11 terrorists took as much pleasure and pride in the fact that their attacks resulted in billions of dollars in financial losses as they did in the world’s reaction to the horror of this staggering one event loss of life. A cyber attack on a number of financial institutions would be "cleaner"—few (if any) deaths, but potentially catastrophic financial losses and disruptions of economic life that could cripple the country. Furthermore, hackers can carry out attacks from secret locations with relatively little financial cost to the terrorist operation.

The Director of the Federal Bureau of Investigations, and heads of DHS and the National Counterterrorism Center told Congress in November 2013 that cyber threats are now a more serious threat to the United States than another 9/11-style attack, because "there are no safe neighborhoods. All of us are neighbors [online]." Former Secretary of Defense Leon Panetta has stated that a cyber attack perpetrated by nation states or rogue violent extremists groups could be as destructive as the attack on 9/11. In light of this, the Senate Intelligence Committee, with strong bipartisan support, recently recommended passage of the Cyber Information Sharing Act which would encourage companies to exchange information with the government on hacking attempts and cyber security threats.

The financial industry has also recognized the cyber attack threat. Major Wall Street firms (through the trade group Securities Industries and Financial Markets Association ("SIFMA") recently proposed the formation of a joint government-industry "cyber war council" to protect financial networks from cyber attacks. The concern is that, because financial markets are now so dependent on the electric grid, any cyber attacks which knock down the power grid and wipe out electronic account data could cause widespread panic which could then lead to a loss of investor confidence and bank runs. Financial firms believe that the systemic consequences of an attack could be devastating for the economy. A cyber attack on a major bank could result in the bank's failure, requiring the Federal Deposit Insurance Corporation ("FDIC") to step in and cover depositors' losses.

The threat of an attack has advanced well beyond the theoretical. "The Mask" cyber attack which specifically targeted domestic natural gas and oil companies was discovered in early 2014 after having gone undetected for more than five years. Security experts at Kapersky Labs described the Mask as the most sophisticated cyber threat ever seen. Beginning in the fall of 2012 and lasting for weeks, hackers conducted denial-of-service ("DOS") attacks on several major bank websites which threatened those institutions' abilities to carry out day-to-day
functions during that time. Security experts believe that hackers are developing variants of the Stuxnet virus, used by the United States to disrupt the Iranian nuclear program, to in turn mount their own attack on American business interests at home and abroad.

The threat of a cyber attack is not limited to the geographic area decimated by a bomb blast. Some opponents of TRIA reauthorization have suggested that the risk of a "traditional" attack is realistically limited to major political, financial and population centers of the country such as Washington, New York and Los Angeles, so that the majority of the country would not be affected and should not have to participate in reinsuring losses to those areas. A cyber attack on a financial institution operating on a nationwide basis, or a broad and concerted attack on local and regional banks across the country may not have such a limited effect, however. Such attacks could wipe out companies' assets all over the United States and affect millions of customers nationwide.

**Cyber Attacks Present the Insurance Industry With an Additional New Risk that It Is Still Struggling to Understand.**

Opponents of TRIA reauthorization argue that the insurance industry has had sufficient time since the 9/11 attacks to create risk models which should accurately gauge the threat of a terrorist attack and allow insurers and insureds to price terrorism coverage accurately. However, the questions raised about TRIA’s coverage of cyber terrorism have not yet been a significant part of the Congressional debate. That discussion has focused almost entirely on the more traditional property and casualty coverages for tangible "property damage" and "bodily injury," coverages that insurers, underwriters and brokers have been analyzing for many years.

The "cyber" element of a cyber terrorist attack adds a large dose of uncertainty to the mix. Relative to other types of claims, insurers have very little experience with cyber-related issues. In response to the comparatively few cyber-related claims asserted over the past two decades, insurers have uniformly taken the position that their standard form general liability and property policies do not provide coverage for losses arising from cyber attacks.

Beginning in the early 2000s, the insurance industry began offering separate coverage for cyber risks such as data theft and loss. Because few insurers or insureds understood the risk and potential damage caused by such losses, coverage for cyber risk insurance was limited at best for most of the last decade.

Within the last few years, however, insurers and brokers have reported that demand for cybersecurity insurance coverage has skyrocketed. Highly publicized events such as the Neiman Marcus data breach in 2012, the Target data breach in 2013, and the eBay data breach in 2014 have highlighted the need for coverage specifically tailored to the threat of cyber attack and its resulting costs. The Center for Strategic and International Studies estimated in June 2014 that cyber crime now costs the global economy over $400 billion each year.

Insurers and brokers have looked to the new cyber risk coverage as an answer to that threat. As a result, the cyber insurance market is expected to almost double from $1 billion in gross written premiums paid last year to as much as $2 billion this year. Most insurers offer
coverage that responds to claims brought against the insured by third parties allegedly damaged by an attack on the insured's networks; these claims contend that the insured is liable to the third parties because of the cybersecurity breach. Insurers generally also offer “first party” cyber coverage which applies to claims by the insured itself for losses suffered because of an attack on the insured's networks. Typical first-party policies cover costs incurred by the insured as a result of the interruption of its business caused by the breach, the costs of remediating the security flaw that led to the breach, and the costs of restoring any data or programs lost or damaged as a result of the breach.

As with terrorism insurance, insurers and brokers are responding to cyber risks that are quite new and very different from the typical perils and risks that they have underwritten for decades. Insurers and brokers admit that they are having difficulty identifying and assessing cyber risks simply because they do not have the necessary experience and concomitant expertise in handling the new phenomenon of cyber attacks. Although there have been several highly publicized data breaches, the targets of those attacks have been reluctant to share information about the details of those events and the pre-breach state of their affected networks; this information would be valuable to underwriters' security experts to assess risks posed to other companies seeking cyber insurance. It appears to be the consensus among insurers and brokers that there is as yet insufficient actuarial data available upon which insurers can create risk models. Underwriters therefore may not have sufficient expertise in cyber security to price cyber risk policies accurately or to identify high-risk companies.

A cyber terrorist attack of the scale feared by SIFMA or DHS could therefore cause huge economic losses that the insurance industry, despite its best efforts, has been unable to adequately address simply because it is faced with two significant new threats: cyber attacks and large-scale terrorist operations. The fledgling cyber insurance sector appears motivated to develop expertise to confront the electronic threats because (1) inaccurate underwriting could result in huge losses to the insurers; and (2) accurate underwriting will help insurers capitalize on the burgeoning cyber insurance demand. A TRIA backstop in the form of reinsurance for primary and excess cyber insurance coverage would serve the dual purpose of protecting insurers and the businesses they insure in the event of a serious terrorist attack, and encouraging insurers to enter and stay in the cyber insurance market despite all the uncertainties.

**TRIA's Current Language Need Not Be, But May Well Be, the Subject of an Ambiguity Debate.**

Some argue that TRIA does encompass coverage for cyber losses. Others assert that TRIA does not specifically address that category of loss. This needless, risky and potentially paralyzing debate should be resolved now in the TRIA reauthorization process. What are the issues to be addressed?

The terms "cyber," "network," "internet," "electronic," "data," and even "computer" do not appear anywhere in the statute. One Congressional conference committee report from the 2002 TRIA enactment process indicates that certain members stated that TRIA applies to cyber events. Legislative history from the 2002, 2005 and 2007 debates about TRIA enactment and reauthorization indicates that Congress did not discuss cyber issues at all.
The question then is whether the statutory language can be read to cover cyber losses. The statute is arguably ambiguous on the issue. TRIA applies to a certified "act of terrorism" which is defined to be "a violent act or an act that is dangerous to (I) human life; (II) property; or (III) infrastructure." One could argue that a cyber attack on banking networks is an attack on the financial "infrastructure" of the United States economy. Also, attacks on energy and telecommunications networks could pose dangers to "human life" through the disruption of energy, health care and law enforcement delivery systems. For example, an attack on a utility's network which results in power loss across a region might cause the deaths of infirm patients dependent on life support machinery. Because the statute does not limit "property" to "tangible property," it is also arguable that electronic data and software are "property" which could be put in danger by a cyber terrorist attack.

On the other hand, it is reasonably arguable that a cyber attack on a telecommunications network which does not actually endanger human life or cause any actual damage to tangible "property" cannot be certified as an "act of terrorism" under TRIA's current language. It also could be argued that the statute applies only to physical infrastructure (such as roads and bridges), and not to intangible infrastructure such as a company's internal computer networks. Thus, thousands of companies may incur huge monetary losses as a result of business interruption directly related to widespread financial network disruption or power loss caused by a cyber attack, yet these losses may not be covered under TRIA because no danger to human life, property or infrastructure arose.

TRIA also applies only to losses under "property and casualty insurance" which is defined as "commercial lines of property and casualty insurance, including excess insurance, workers' compensation insurance, and surety insurance." "Property and casualty insurance" is specifically defined to exclude from TRIA's coverage crop insurance, private mortgage insurance, financial guaranty insurance, medical malpractice insurance, life or health insurance, flood insurance or reinsurance. Many types of currently available cyber coverages fall within professional liability/errors & omissions lines of coverage or directors and officers coverages, neither of which is explicitly included within TRIA.

Some have also raised the issue of whether TRIA's geographic limitations will prevent it from applying to cyber attacks. TRIA applies in relevant part only to an "act of terrorism" that has been certified "to have resulted in damage within the United States." "Damage" is not defined and could be interpreted broadly to apply to any "loss" incurred by businesses located in the United States, regardless of whether it is loss of intangible data or physical harm to tangible property. A cyber attack on networks maintained by foreign corporations in foreign countries which results in the loss or destruction of vital financial information could have a significant effect on American businesses and their customers such that "damage within the United States" resulted even though the terrorist activity took place abroad.

The current state of affairs is that cyber coverage is arguably neither specifically included nor generally excluded from coverage under TRIA, which adds to the uncertainty surrounding this issue. Could a strong argument be made that TRIA applies to cyber losses? Some interested parties appear willing to rely on the existing statutory language for the position that TRIA covers...
cyber terrorism losses. Senator Jack Reed attempted to aid this line of thinking by stating on the record during the Senate's consideration of S. 2244 that cyber terrorist attacks "would continue to fall within the scope of TRIA's covered lines, as they do today." Senator Reed's comments combined with the legislative record from 2002 may help a court decide that TRIA as it currently exists must be applied to losses caused by cyber terrorist attacks.

However, some judges adhere to a strict "textualist" theory of statutory interpretation. Under this theory, courts should apply only the "plain language" of the statute and should not try to divine the legislature's intent by looking to legislative history or other extra-statutory sources. The mere fact that TRIA as presently written does not discuss cyber-related issues may be sufficient grounds for a textualist judge to limit TRIA's reach, notwithstanding any comments in TRIA's legislative history declaring that the statute should be read to apply to cyber attacks.

Congress Should Clarify That TRIA Applies to Cyber Attacks.

The lack of any explicit reference to cyber attacks in TRIA should be at least troubling to Congress given the magnitude of the threat. As discussed above, cyber terrorism is now considered to pose the most imminent and significant terrorism risk to the United States. Should a cyber terrorist attack occur, a strict textualist court could conceivably find that TRIA does not apply to cyber terrorism at all, leaving the business and the insurance industry without any backstop whatsoever. If Congress intends that cyber attacks should fall within TRIA's ambit, it should amend TRIA to eliminate any doubt.

To fully protect businesses from this most imminent threat, Congress should assure that TRIA apply to cyber attacks. Any limitation of TRIA's reach to physical losses would ignore what government and business leaders believe to be the direst risk of terrorist attack. None of the bills pending in Congress address cyber terrorism. Commentators have raised the legitimate concern that injecting cyber issues into the debate in a very partisan environment—even if it is just to reemphasize that TRIA applies to cyber issues—will complicate matters given the short amount of time Congress has to consider TRIA reauthorization before the statute expires in December 2014.

It should be noted here that TRIA is intended to provide a backstop only where a primary and/or umbrella insurance policy provides coverage for the loss. Whether there is coverage for damages caused by cyber attacks under standard form general commercial liability and property policies is a question still being resolved by courts. Standalone cyber insurance policies, which are only now becoming widely used, are specifically designed to cover cyber attacks. If TRIA were specifically expanded to encompass any policy type—general liability, E&O, D&O or specific peril cyber liability or first party cover—it could provide a backstop so long as it is clear that each of those policies is governed by TRIA's current "make available" provisions. Thereafter, TRIA cyber risk coverage would be afforded to businesses that responsibly go out and purchase coverage protecting them from the growing cyber threat. Businesses careful enough to protect themselves from cyber threats by purchasing this insurance, and their insurers that are willing to underwrite this coverage despite all of the uncertainty it poses, should be protected. The premium base that would follow would add to the industry's reserves and increase the surplus available for loss.
Interested parties have raised the valid political concern that there is little appetite in the current hyper-partisan climate to "expand" TRIA to cover cyber attacks. Applying TRIA to cyber attacks does not change the cost of the backstop, as the federal government's reimbursement to insurers for damages resulting from a certified "act of terrorism" will remain capped at $100 billion. Thus, a terrorist attack which is entirely electronic in nature will cost the Treasury no more than another 9/11-style event.

Our government is now very aware of the cyber terrorist threat. Elimination of cyber vulnerabilities is a high priority of federal agencies and business interests. Electronic information networks are as critical to the operation and survival of American businesses as the brick-and-mortar buildings which are already protected under TRIA. TRIA's renewal is on the Congressional agenda this fall, and cyber coverage should be included in the debate while both issues are on everyone's minds.

4 Banks Dreading Computer Hacks Call for Cyber War Council, Bloomberg.com (7/8/14).
7 Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime (June 2014).
8 Insurers in Dash for Expertise to Master Cyber Risk Insurance, Insurance Journal (7/14/2014).
9 TRIA, § 102(1)(A).
10 TRIA, § 102(12).
11 TRIA, § 102(1)(A)(iii).
12 Cyberattack Questions Emerging in TRIA Reauthorization Bill Debate, Bloomberg BNA (7/18/2014).