CYBER AND TRIA: EXPANDING THE DEFINITION OF AN "ACT OF TERRORISM" TO INCLUDE CYBER ATTACKS

NEHAL PATEL†

ABSTRACT

The 9/11 terrorist attacks brought on financial losses that caused insurers and Congress to reevaluate how the United States approaches terrorism risk coverage. Congress quelled concerns of insurers evading coverage of future terrorist attacks by enacting the Terrorism Risk Insurance Act in 2002. This Note considers the difficulties presented by the out-of-date language employed by Congress in 2002 and proposes amendments so that the Act more clearly covers acts of cyberterrorism, which are ever-growing in their destructive potential.

INTRODUCTION

The tragic events of September 11, 2001 caused panic throughout industries in the United States. The insurance industry experienced direct financial pain. Due to the high insurance payouts[1] from claims based on the September 11 attacks, insurers reevaluated their position, ultimately deciding the extremely high expected payouts and low predictability made terrorism risk insurance almost impossible to cover comfortably. Congress responded by enacting the Terrorism Risk Insurance Act of 2002 ("TRIA"),[2] which created a federal program designed to facilitate reinsurance for terrorism risk. Thereafter, insurers were required to participate in the program and insure terrorism risk. The newly created program has yet to be activated, as the U.S. has not been subject to another catastrophic terrorist attack the level of the September 11 attacks.

New terrorist groups have emerged that are focused on cyberwarfare and cyberterrorism. Even though cyberattacks are more common now, Congressional reauthorization in 2007, 2015, and 2019 left TRIA's language unchanged. This paper argues that TRIA's language leaves ambiguity as to when the Secretary of the Treasury ("Secretary") must certify a cyberattack as an act of terrorism. This ambiguity creates dangerous regulatory uncertainty for both insurers and the insured, as the Secretary's certification determines an insurer's decision to cover the event.

---

† Duke University School of Law, J.D. expected May 2021.

[1] Insurance losses totaled $39.5 billion in U.S. dollars adjusted to 2008 dollars. *9/11 and Insurance: The Eight Year Anniversary - Insurers Paid Out Nearly $40 Billion*, INSURANCE INFORMATION INSTITUTE (Sept. 10, 2009), https://www.iii.org/press-release/9-11-and-insurance-the-eight-year-anniversary-insurers-paid-out-nearly-40-billion-091009.

[2] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, § 201, 116 Stat. 2337.

TRIA was reauthorized in December 2019.[3] In such reauthorization, Congress extended the program until 2027, requesting Treasury research the effectiveness of the program in regards to cyberterrorism.[4] Congress should have gone one step further by explicitly including cyberattacks as an act of terrorism.

I. BACKGROUND: TERRORISM RISK INSURANCE

A. Pre-September 11 Attacks

Before September 11, 2001, terrorism risk insurance coverage was widely available. Since the 1930s, personal and commercial property insurance increasingly covered all risks of property loss, called all-peril coverage.[5] Under all-peril coverage, insurers would compensate property losses regardless of the cause.[6] The all-peril coverage eventually turned into general package policies, which came with certain exceptions, such as acts of war.[7] By 1995, 93% of all homeowners' policies were all-peril with explicitly stated limited exceptions.[8] Acts of war were often an exception to coverage because acts of war are inherently catastrophic and can drain all the capital from insurers in a single event.[9] Although acts of terrorism seem to parallel acts of war by causing similarly high losses, acts of terrorism were not among the exceptions in property insurance coverage.[10]

The inconsistency in insurance coverage treatment can be attributed to general ignorance, due to extremely low probability and difficulty in defining "acts of terrorism."[11] Before 9/11, insurers simply did not consider terrorism attacks a credible threat, despite the 1993 World Trade Center bombing and the 1995 Oklahoma City bombings.[12] Notably, many other countries' insurance policies explicitly excluded terrorism risk due to increased terrorist activities in the 1970s and 1980s.[13] Although many foreign insurers noted and addressed terrorism risk, insurers in the United States neglected any concern for terrorism risk.

---

[3] Terrorism Risk Insurance Program Reauthorization Act of 2019, H.R. 1865, 116th Cong. § 501 (2019).

[4] H.R. 1865, § 502. The research conducted by Treasury, published in April 2020, indicated ambiguity and confusion as will be explained in this Note. *See* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, TERRORISM RISK INSURANCE: MARKET IS STABLE BUT TREASURY COULD STRENGTHEN COMMUNICATIONS ABOUT ITS PROCESS (2020).

[5] Howard Kunreuther & Mark Pauly, *Terrorism Losses and All Perils Insurance*, 23 J. INS. REG. 3, 5 (2005).

[6] *Id.*

[7] *Id.*

[8] *See id.* (noting commercial property coverage likely was almost exclusively all-peril, as commercial property coverage mirrored personal property coverage).

[9] *Id.* at 6.

[10] *Id.* at 5.

[11] *Id.* at 9, 11.

[12] *Id.* at 7, 11.

[13] *Id.* at 10, 11.

Additionally, acts of terrorism took many forms and came from many sources. The United States had yet to recognize a legal definition of an "act of terrorism."[14] Further, typical act of war exclusions disclaimed coverage over "large losses from war and *correlated warlike activities*."[15] Insurers may have assumed all attacks against the United States that caused extremely large monetary losses would fall under the act of war exclusion. However, in the only pre-2001 case challenging the denial of an insurance claim based on an act of war exclusion, the Second Circuit denied an insurer the right to claim an act of war exclusion on a plane destroyed by terrorists.[16] By September 11, 2001, terrorism risk was insured as an afterthought to general property insurance coverage.[17]

B. Introduction to Terrorism Risk Insurance Act & Terrorism Risk Insurance Program

On September 11, 2001, terrorists caused about 3,000 deaths[18] and about $22 billion in property damage.[19] In total, an estimated $35 billion to $75 billion in monetary losses were suffered.[20] As a result, insurance providers were expected to make heavy payouts on claims against the attacks.[21] Reinsurers were expected to compensate primary insurers for the payouts.[22] Insurers and reinsurers had no choice. Not only would the American public and leaders have ostracized insurers who considered rejecting claims on the September 11 attacks,[23] but the only court case related to the issue was resolved in favor of the insured.[24]

Although a terrorist attack against the United States was not surprising, the American people and insurers were stunned by this attack's devasting losses.[25] The monetary losses suffered were the highest of any

---

[14] *Id.* at 11.

[15] Richard Allyn & Heather McNeff, *The Fall and Rise of Terrorism Insurance Coverage Since September 11, 2001*, 29 WM. MITCHELL L. REV. 821, 823 (2003) (emphasis added).

[16] *See* Pan American World Airways, Inc. v. Aetna Casualty & Surety Co, 505 F.2d 989, 1009–22 (2d Cir. 1974) (holding the doctrine of *contra proferentem* applies in this case because many terms in the exclusions were not judicially defined).

[17] *See id.*

[18] Allyn & McNeff, *supra* note 15, at 826.

[19] Adam Z. Rose & S. Brock Blomberg, *Total Economic Consequences of Terrorist Attacks: Insights from 9/11*, 16 PEACE ECONOMICS, PEACE SCIENCE AND PUBLIC POLICY 1, 6 (2010).

[20] *See* Allyn & McNeff, *supra* note 15, at 826. *See also*, Kunreuther & Pauly, *supra* 5, at 4 (estimating insurance losses at $40 billion).

[21] *See* Allyn & McNeff, *supra* note 15, at 827 (citing the U.S. House Financial Services Committee letter stating that "it would be unpatriotic of insurers to try to avoid coverage of the attack based on 'legal maneuvering'").

[22] Kunreuther & Pauly, *supra* note 5, at 11.

[23] *See* Allyn & McNeff, *supra* note 15, at 827 (noting that Congress wrote a letter directed at insurers, which stated "that it would be unpatriotic of insurers to try to avoid coverage of the attack based on 'legal maneuvering'").

[24] *Pan American World Airways*, 505 F.2d 989, 1009–22 (2d Cir. 1974).

[25] *See* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL

disaster in United States history.[26] The Congressional Research Service estimated the 9/11 attacks were the largest insurance loss from a terrorist attack, totaling $26.22 billion in property insurance losses.[27] For reference, the next twenty largest attacks totaled $6.55 billion in property insurance losses.[28] Insurers responded to the September 11 attacks by adding terrorism exclusions to new and renewed property and casualty insurance.[29] This new policy effectively protected insurers from paying certain claims against future terrorist attacks.[30] The National Association of Insurance Commissioners ("NAIC") and most states approved the new terrorism risk exclusion.[31] By February 2002, 45 states, the District of Columbia, and Puerto Rico, had approved the exclusion.[32] Under these state-approved exclusions, if terrorists attacked the United States, ordinary citizens would have to pay for the damage sustained.[33]

Fearing the lack of terrorism risk coverage would be a significant factor in business decisions, particularly lending,[34] Congress enacted the Terrorism Risk Insurance Act, signed into law by President Bush on November 26, 2002.[35] TRIA created the Terrorism Risk Insurance Program ("TRIP"), a federal loss-sharing program for terrorism risk insurance coverage.[36] TRIP requires insurers make terrorism risk coverage available for all property and casualty insurance policies for all consumers.[37] For example, if a homeowner has a car, insurers must offer terrorism risk insurance for both the homeowner's auto and home insurance policies. This coverage requirement applies to all property and casualty policies.

Insurers offer terrorism risk insurance at an average of 2.5 to 3.0 percent of the total premium.[38] Often, terrorism risk insurance is included

---

COMMISSION ON TERRORIST ATTACKS 174–214 (2004) (detailing the multiple attacks planned or conducted against the United States by Islamic extremists and growing animosity against the United States in the decade leading up to the September 11th attacks).

[26] *See* Robert H. Jerry, II, *Insurance, Terrorism, and 9/11: Reflections on Three Threshold Questions*, 9 CONN. INS. L.J. 95, 105 (2002) (noting that before the September 11th attacks, Hurricane Andrew was the largest insured disaster in United States history, which caused $16 billion in losses and was, to some degree, predicted).

[27] CONGRESSIONAL RESEARCH SERVICE, THE TERRORISM RISK INSURANCE ACT (TRIA) 1 (last updated Feb. 1, 2019).

[28] *Id.*

[29] Allyn & McNeff, *supra* note 15, at 828.

[30] *Id.*

[31] *Id.* at 830.

[32] *Id.*

[33] *Id.*

[34] CONGRESSIONAL RESEARCH SERVICE, *supra* note 27.

[35] Allyn & McNeff, *supra* note 15, at 828.

[36] *Background on: Terrorism risk and insurance*, INSURANCE INFORMATION INSTITUTE (Dec. 16, 2019), https://www.iii.org/article/background-on-terrorism-risk-and-insurance.

[37] *Id.*

[38] Federal Insurance Office, *Report on the Effectiveness of the Terrorism Risk Insurance Program*, U.S. DEPARTMENT OF THE TREASURY, 25 (June 2018).

in policies for no extra cost.[39] As of 2017, about 70–80% of consumers have purchased terrorism risk insurance.[40] Under TRIP, insurers must pay the claims on certified acts of terrorism for those consumers while the federal government provides a federal backstop that allows insurers to reclaim the payments through higher future premiums across the board.[41] Since 2001, many terrorist attacks have occurred;[42] however, none of the terror attacks have been certified as an act of terrorism for TRIP purposes.

C. Cyberspace

1. Cyberattacks in the United States

Cyberattacks have been around since the 1980s.[43] As the internet use skyrocketed in the 1990s and turn of the century, cyberattacks became sophisticated, enabling attackers to steal valuable data[44] and destroy computer infrastructure.[45]

Hacking has resulted in hundreds of millions of financial losses. In 2007, hackers from the United States, Eastern Europe, and China stole 45,700,000 credit and debit card numbers, eventually resulting in a $130 million settlement.[46] The hack has reportedly affected an additional 48 million people.[47] In 2008, hackers stole customer data from Internet Auction, one of Korea's largest Internet shopping sites.[48] About 10.8 million customers were affected by the Internet Auction attack. Hackers stole information from 3 billion Yahoo! accounts in 2013 and another 500 million separately in 2014.[49] These continued hacks "will cost the world $6 trillion annually by 2021," according to Cybersecurity Ventures.[50]

---

[39] *Id.*
[40] *Id.* at 29.
[41] *See id.*
[42] Peter Bergen, Albert Ford, et al., *Terrorism in America After 9/11*, NEW AMERICA (Sep. 18, 2019), https://www.newamerica.org/in-depth/terrorism-in-america/part-i-overview-terrorism-cases-2001-today/.
[43] Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare*, 1 J.L. & CYBER WARFARE 99, 104 (2012).
[44] *See, e.g.*, *id.* at 111–12 (describing the cases of Kevin Poulsen and Kevin Mitnick).
[45] *See, e.g.*, Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[46] Tiffany Gates & Katy Jacob, *Payments Fraud: Perception Versus Reality – A Conference Summary*, 32 ECON. PERSPECTIVES 1, 7 (2009).
[47] *Id.*
[48] MinJae Lee & JinKyu Lee, *The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet*, 14 Inf. Syst. Front. 375, 375 (2012).
[49] Soo Youn, *The Capital One data breach is alarming, but these are the 5 worst corporate hacks*, ABC NEWS (Jul 30, 2019), https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391.
[50] Steve Morgan, *Cybercrime Damages $6 Trillion By 2021*, CYBERSECURITY VENTURES (Oct. 16, 2017), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Some hacking is becoming politically motivated. "Hacktivism" is the recent movement, described by the Department of Justice's National Infrastructure Protection Center, where hacker activists "launch politically motivated attacks on public web pages or e-mail servers."[51]

Hacking to steal information is only one highly destructive form of cyberattack. Recently considered to be "the Most Devastating Cyberattack in History," NotPetya was released by alleged Russian military hackers known as Sandworm in 2017.[52] NotPetya was a piece of malware released into a single company's update servers.[53] Once released, the malware "spread automatically, rapidly, and indiscriminately."[54] Within hours, NotPetya spread from its origin site in Ukraine to computers around the world – from hospitals in the United States to factories in Tasmania – even hitting the Russian state-sponsored oil company, Rosneft.[55] Once in a computer, NotPetya encrypted the master boot records, immediately destroyed the computer's ability to find its own operating system.[56] If a computer cannot find and load its own operating system, it is crippled beyond repair.[57] To jump from computer to computer within a single system, the worm stole the username and password of employees whose credentials could be used to log into multiple computers.[58] Therefore, once in a company's system, NotPetya crippled most company computers, effectively crippling the company's ability to function.[59] Maersk, Merck, TNT Express, Saint-Gobaian, Mondelez, and Rickitt Benckiser were all crippled, each required to pay nine-figures to replace the destroyed machines.[60] In total, the White House estimated more than $10 billion in damage resulted worldwide.[61] Only one month prior to the release of NotPetya, another kind of malware, WannaCry, caused between $4 billion and $8 billion in damage.[62]

2. Cyberterrorism

Cyberspace is an attractive mode of attack for terrorists for several reasons. Terrorists with fewer resources can "target and affect large

---

[51] Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUT. & HIGH TECH. L.J. 177, 183 (2000).

[52] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id. See also* Jonathan Berr, *"WannaCry" ransomware attack losses could reach $4 billion*, CBS NEWS (May 16, 2017), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

numbers of people" with just a computer and internet access.[63] Cyberterrorists can more easily blend into the common population of host states.[64] Specific targeting of weaker, exploitable systems is easier.[65] Once the malware is developed and placed, launching an attack can be instantaneous and sometimes requires no further preparation.[66] Navigating through cyberspace is, in some circumstances, easier to navigate without detection than navigating through physical space.[67]

Despite the appeal, cyberterrorism has only recently become a significant fear with the introduction of the WannaCry and NotPetya attacks.[68] "Traditionally, most cyberattacks have been carried out by criminal organizations," not by terror organizations.[69] WannaCry and NotPetya, which "affected organizations in more than 150 countries" combined, are likely to spur more cyberterrorism activity.[70]

Critical infrastructure is especially sensitive to a terrorist attack. In 2013, then-President Barack Obama issued an executive order addressing critical infrastructure cybersecurity, noting the "cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."[71] Terrorists tend to look to amass the most destruction in a single attack. Malware like WannaCry and NotPetya has the potential to infiltrate and destroy U.S. infrastructure, such as hospital systems or electrical grids, leaving millions vulnerable instantaneously. Although the United States is noting and addressing cybersecurity concerns of critical infrastructure,[72] cyberwarfare is a continually adaptive endeavor.[73]

II. TERRORISM RISK INSURANCE PROGRAM

A. Certification of an Act of Terrorism

For TRIP to be initiated, the Secretary of the Treasury, in concurrence with the Secretary of State and the Attorney General of the

---

[63] Murat Dogrul, Adil Aslan & Eyyup Celik, *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, TURKISH AIR WAR COLLEGE 29, 32 (2011).

[64] *See id.* at 33 ("[Being in a host state] enables terrorists to remain unknown").

[65] *See id.* ("…attacks are easy to carry out because many targets are poorly protected").

[66] *Id.*

[67] *See id.* ("There are no physical barriers or check points that [terrorists] have to cross.").

[68] Emil Metropoulos & Jeremy S. Platt, *Global Cyber Terrorism Incidents on the Rise*, MARSH & MCLENNAN ADVANTAGE, (Nov. 2018), https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

[69] *Id.*

[70] *Id.*

[71] Exec. Order. No. 13636, 78 FR 11739, 11739 (Feb. 12, 2013).

[72] *See generally*, *id.*

[73] *See* Michael Plachta, *Council of Europe Adopts Resolution and Recommendation on Cyberterrorism*, 31 NO. 7 INT'L ENF'T L. REP. 279 (Jul. 2015).

United States, must certify an attack as an "act of terrorism."[74] The Secretary's decision to certify or refrain from certifying an attack is final and "not… subject to judicial review."[75] Certification falls only on the Secretary of the Treasury's shoulders, and may not be delegated "to any other officer, employee, or person . . ."[76] Therefore, only the Secretary of the Treasury can initiate the program, and that initiation is based on a certification that cannot be contested by any party.

TRIA details a four-pronged definition for certification of an 'act of terrorism.'[77] First, the attack must "be an act of terrorism."[78] Second, the attack must be a "violent act or an act that is dangerous to… human life;… property; or… infrastructure."[79] Third, the attack must result in damage within the United States, on an air carrier or vessel, or the premises of a United States mission.[80] Finally, the attackers must have acted "on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion."[81]

If the Secretary of the Treasury certifies an attack as an act of terrorism, the program is subject to a triggering threshold based on total insurance losses from the attack.[82] Originally set at $5 million in 2002, subsequent reauthorizations of TRIA in 2007 and 2015 raised the threshold to $100 million and $200 million, respectively.[83] If an attack has caused more than $200 million in damages and was certified as an act of terrorism for TRIP purposes, insurers must cover claims due to the attack. The program remains in effect up to $100 billion in losses per year.[84] If certified acts of terrorism have caused more than $100 billion in covered losses in a year, the losses above the $100 billion threshold may not be covered by insurers.

---

[74] Fed. Ins. Office, *supra* note 38, at 29.
[75] Terrorism Risk Ins. Act of 2002, Pub. L. No. 107-297, § 102(1)(C).
[76] *Id.* at § 102(1)(D).
[77] *Id.* at § 102(1)(A). In addition to the four-pronged definition, the Act provides an exception to certification if "the act is committed as part of the course of a war declared by Congress." § 102(1)(B). However, Congress last declared a war in 1942, despite the United States engaging in warfare since 1942. United States Senate, *Official Declarations of War by Congress* (2010) https://www.senate.gov/pagelayout/history/h_multi_sections_and_teasers/WarDeclarationsbyCongress.html.
[78] *Id.* at § 102(1)(A)(i).
[79] *Id.* at § 102(1)(A)(ii).
[80] *Id.* at § 102(1)(A)(iii).
[81] *Id.* at § 102(1)(A)(iv).
[82] Ins. Info. Inst., *supra* note 36.
[83] *See* § 102(1)(B)(ii) (disallowing certification of attacks wherein "property and casualty insurance losses resulting from the act, in the aggregate, do not exceed $5,000,000"). *See also*, Terrorism Risk Insurance Program Reauthorization Act of 2007, Pub. L. No. 110-160, 121 Stat. 1839; Terrorism Risk Insurance Program Reauthorization Act of 2015, Pub. L. No. 114-1, 129 Stat. 3.
[84] *See* Ins. Info. Inst., *supra* note 36.

The definition of an act of terrorism under TRIA has not been interpreted by courts for two reasons. First, although there have been many terror attacks since 2001, none have risen to the financial threshold required to be certified.[85] Therefore, there has been no reason to interpret the statute. However, even if TRIP were to be initiated, TRIA specifically denies the courts the ability to adjudicate the Secretary's certification.[86]

Therefore, the somewhat abstract process of certification concerned Congress in light of questions of certifying the Boston Marathon bombing.[87] For clarity purposes, Congress required the Secretary of the Treasury to "conduct and complete a study on the process by which the Secretary determines whether to certify an 'act of terrorism' under TRIA…"[88] The Department of the Treasury ("Treasury") fulfilled that request by issuing a report in October 2015 on TRIP Certification.[89] The report focused on the procedure of efficiently certifying, rather than the substance of certification.[90]

The Treasury explained three "general criteria" required for certification, which traced the second, third, and fourth prongs of the definition of an "act of war" under TRIA.[91] Under Treasury's general criteria, first, the act must "be a violent act or an act that is dangerous to human life, property, or infrastructure…"[92] Second, the attack must "have resulted in damage within the United States."[93] Finally, the act must "have been committed by an individual or individuals, as part of an effort to coerce the civilian population of the United States or influence the policy or affect the conduct of the United States Government by coercion."[94] Treasury noted the first and third criteria posit "a number of potential permutations" and add to the "complexity of the certification analysis."[95]

---

[85] In April 2013, the Boston Marathon bombing, which President Barack Obama called an "act of terror," resulted in less than $5 million in damages, according to the Massachusetts Department of Insurance. Baird Webel, *Terrorism Risk Insurance: Issue Analysis and Overview of Current Program*, Congressional Research Service, 2 (July 23, 2014). The Boston Marathon bombing was "one of the highest-profile attacks on U.S. soil since Sept. 11, 2001," killing three people and wounding 260 others. Nate Raymond, *Boston Marathon bomber appeals conviction, death sentence*, REUTERS (Dec. 27, 2018), https://www.reuters.com/article/us-boston-bombings-appeal/boston-marathon-bomber-appeals-conviction-death-sentence-idUSKCN1OQ1F4.

[86] *See* Terrorism Risk Ins. Act of 2002 § 102(1)(C).

[87] *See* Terrorism Risk Ins. Program Reauthorization Act of 2015 § 107.

[88] U.S. DEPARTMENT OF THE TREASURY, THE PROCESS FOR CERTIFYING AN "ACT OF TERRORISM" UNDER THE TERRORISM RISK INSURANCE ACT OF 2002, (Oct. 2015).

[89] *See generally, id.*

[90] *See generally, id.*

[91] *Id.* at 5. The general criteria excluded the first prong that the attack be an act of terrorism, as Treasury found this prong to be circular and therefore did not add anything to the analysis.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

B. Applying TRIA to Cyberattacks

The undisputable discretion given to the Secretary of the Treasury presents legal issues. First, without legal precedent or guidance on certification, the Secretary's decision to certify an attack can fall on arbitrary judgments. Second, as the Secretary's decision is final, certification of an act of terrorism is fully removed from the President's Article II powers. The only guidance published by Treasury on certification of an act of terrorism reiterated the definition of an "act of terrorism" without laying out a method of analyzing the definition."[96] The public and insurers are left guessing how the Secretary of the Treasury will interpret TRIA's definition of an "act of terrorism" without useful guidance from Treasury or Congress.

1. The Search for a Violent or Dangerous Act in Cyberspace

The Secretary would first have to determine whether the attack is a violent act or at least one dangerous to human life, property, or infrastructure. For an act to be violent, it must be "marked by the use of usually harmful or destructive physical force."[97] Cyberattacks are not typically thought of as physical, but there are physical aspects of a cyberattack. The attackers are moving through cyberspace – a non-physical medium – and may be attacking a non-physical system, such as a hospital electronic medical record system or an electrical grid. However, some bugs may be created that can overheat computers, crashing computers through use of some harmful physical force.[98] Whether an attack is dangerous to human life, property, or infrastructure is highly factual. Unlike a physical attack, where material weapons are used to destroy property cyberattacks may take many forms and produce many outcomes, some of which are far from physical.

Stealing data may be dangerous to human life, but only if the data is highly sensitive. For example, if a piece of data suggests the location of a United States spy abroad, a hacker who illegally obtains that piece of data by means of a cyberattack may fall under the first of the three general criteria. However, this one piece of data may be hidden in a mountain of stolen data. The hacker may not even know what data was obtained. The Secretary may similarly be unaware. For the Secretary to make a determination of dangerousness to human life, the Secretary must not only know exactly what data was stolen, but also what inferences may be made based on the data, and how those inferences may be used to threaten U.S. lives.

Data may also be seen as a form of property. If so, stealing data owned by a U.S. person or business is inherently dangerous to property. However, it is unclear whether TRIA was intended to protect this type of

---

[96] *See generally*, *id.*

[97] *Violent*, Merriam-Webster Dictionary (11th Ed. 2019).

[98] Hamilton Turner, et al., *Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?*, 41, IEEE Computer and Reliability Societies (May/June 2015), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7118094.

property. Congress neglected to define "property" under TRIA.[99] And "basing the definition of 'property' on a judgment call…allows the government's interests to warp the private rights" of U.S. citizens.[100] TRIA gives Secretary of the Treasury unopposed unilateral discretion in determining how to define property. When considering the definition of 'property' under the Bankruptcy Act, the Supreme Court has noted "the most important consideration limiting the breadth of the definition of 'property' lies in the basic purpose of the Bankruptcy Act…"[101] The Court looked to the Act's framers' intent to determine purpose.[102]

The framers of TRIA did not explicate an interest in a certain type of property. However, the framers enacted TRIA a year after the September 11 attacks. TRIA was effectively a Congressional response to state-approved terrorism risk exclusions after the September 11 attacks.[103] The stated purpose of the Act did not point to a certain type of property, but rather focused on providing property and casualty insurance.[104] So the framers' definition of "property" may be derived from what is covered under property and casualty insurance. Cyber liability falls under property and casualty insurance.[105] However, typically cyber insurance policies contain exclusions, including intellectual property,[106] data breaches,[107] and common physical causes of computer crashes.[108] For example, the standard commercial property policy excludes perils caused by power surges, electrical disturbances, temperature changes, and mechanical

---

[99] *See generally*, Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322.

[100] Murr v. Wisconsin, 137 S.Ct. 1933, 1957 (2017) (Roberts, J., dissenting).

[101] Lines v. Frederick, 400 U.S. 18, 19 (1970) (citing Local Loan Co. v. Hunt, 292 U.S. 234, 244 (1934)).

[102] *Id.* (citing Swarts v. Fourth Nat'l Bank, 117 F. 1, 3 (8th Cir. 1902)).

[103] *See* Allyn & McNeff, *supra* note 15, at 828.

[104] *See* Terrorism Risk Insurance Act at § 101(b) (stating the purpose of the Act was "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"); *Id.* at § 101(b)(1) (stating the program was designed to "protect consumers by addressing market disruptions and ensure the continued widespread availability and affordability of property and casualty insurance for terrorism risk").

[105] *See* Summit Insurance Services, *Property and Casualty* https://www.summitinsuranceservices.com/services/property-and-casualty/ (advertising property and casualty coverage, including "newer products such as cyber liability insurance").

[106] Dan Burke, *Cyber Insurance 101: What Cyber Insurance Covers, 2020*, WOODRUFF SAWYER (2019), https://woodruffsawyer.com/cyber-liability/cyber-basics/.

[107] Catherine Del Prete, *Common Exclusions Invoked by Cyber Carriers to Deny Coverage*, PERKINS COIE: TECH RISK REP. (2019) https://www.techriskreport.com/2019/02/common-exclusions-invoked-cyber-carriers-deny-coverage/.

[108] *See* Marianne Bonner, *Coverage For Computers and Data Under a Commercial Property Policy*, THE BALANCE SMALL BUSINESS: BUSINESS INSURANCE, (Nov. 29, 2019) https://www.thebalancesmb.com/commercial-property-policy-computers-and-data-462677.

breakdown.[109] The standard policy's exclusions are all typical methods malware, like NotPeyta and WannaCry, destroy computers.

As TRIA requires insurers to provide terrorism risk insurance for all covered property and casualty insurance, these exclusions are problematic for certifying a cyberattack on the basis that the attack is dangerous to property for two reasons. First, if the Secretary of the Treasury defines property by the purpose of the Act, property does not include stolen intellectual property, stolen data, or destroyed computers. The purpose of the Act makes clear property is defined by property and casualty insurance coverage. Indeed, Congress limited TRIP certification based on a threshold of aggregate property and casualty insurance losses.[110] And Congress further defined "insured loss" as "losses resulting from an act of terrorism…that is covered by primary or excess *property and casualty insurance*."[111] So the exclusions provide a safeguard for insurers in the event the Secretary of the Treasury intends to certify a cyberattack that falls under an exclusion.

Second, insurers are allowed to apply exclusions to claims. Nothing in TRIA overrides exclusions.[112] By only attaching TRIP-required payments to active property and casualty insurance claims,[113] Congress implicitly allowed insurers to forego payments on any types of terror attacks as long as insurers excluded coverage for that type of claim under all circumstances. For example, active act of war exclusions still apply to policies. If a hostile state attacks the United States, insurers would not pay claims, nor be expected to pay claims, due to act of war exclusions.[114]

Although the aforementioned exclusions would also be applied narrowly to cyber risk insurance policies, such exclusions would likely hold. Courts tend to construe insurance policies narrowly.[115] Under the doctrine of *contra proferentem*, any ambiguity in an exclusion is generally construed against the insurer and in favor of the insured."[116] *Contra proferentem* especially applies when insurers know the language in their

---

[109] *Id.*

[110] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, § 102(1)(B)(ii), 116 Stat. 2322, 2324.

[111] *Id.* § 102(5) (emphasis added).

[112] *See* Terrorism Risk Insurance Act of 2002 at *passium*.

[113] *See id.* at § 101(b).

[114] Note, Act of War exclusions are sometimes referred to as Hostile Acts exclusions or War Risk exclusions. Michael Menapace, *Property Insurance, Cyber Insurance, Coverage and War: Losses From Malware May Not Be Covered Due to Your Policy's Hostile Acts Exclusion*, THE NAT'L L. REV., (Mar. 10, 2019), https://www.natlawreview.com/article/property-insurance-cyber-insurance-coverage-and-war-losses-malware-may-not-be-0.

[115] *See, e.g.*, Netherlands Insurance Company v. Phusion Projects, Inc., 737 F.3d 1174, 1177 (7th Cir. 2013); Nautilus Ins. v. Country Oaks Apartments Ltd., 566 F.3d 452, 454–55 (5th Cir. 2009); Twin City Fire Ins. v. Ohio Cas. Ins., 480 F.3d 1254, 1263 (11th Cir. 2007).

[116] Universal Cable Productions, LLC v. Atlantic Specialty Ins. , 929 F.3d 1143, 1151 (9th Cir. 2019) (citing Garcia v. Truck Ins. Exch., 682 P.2d 1100, 1106 (Cal. 1984)).

policies are ambiguous.[117] However, courts only apply *contra proferentem* in cases of ambiguous exclusions.[118] So, if insurers have reason to make the language in such exclusions as exact as possible, courts will not have reason to apply *contra proferentem* against insurers. Recently policyholders have won cases in which insurers rejected claims based on intellectual property exclusions.[119] There is a growing body of caselaw against these standardized exclusions, forcing insurers to more precisely define their exclusions. So, even if claims are submitted on a TRIP-certified act of terrorism, the exclusions would likely apply.

The final prong of the first criteria presents a similar issue, as "infrastructure" is not defined by the statute.[120] In fact, "infrastructure" is not mentioned again in the statute.[121] Courts have not defined the term "infrastructure," but under the same logic as the second prong, network infrastructure may be protected under TRIA. Cyber insurance typically includes network security and privacy liability, which covers "data breach, malware infection, cyber extortion demand, ransomware, [and] business email compromise."[122] These are typical of cyberattacks. At the time of TRIA enactment, Congress was likely considering physical U.S. infrastructure, such as building, bridges, and electric power grids. However, by setting the purpose of the Act in terms of property and casualty insurance, Congress may have given rise to terrorism risk coverage for any type of network infrastructure, including business network systems. Therefore, the Secretary may be able to determine a terrorist hack is dangerous to infrastructure.

Certification of more destructive types of cyberattacks, such as NotPetya, would be easier to justify.[123] NotPetya was designed to, and did, destroy computers owned by U.S. businesses, hospitals, and

---

[117] Pan American World Airways, Inc. v. Aetna Casualty & Surety Co, 505 F.2d 989, 999 (2d Cir. 1974).

[118] *See* Hugo Boss Fashions, Inc. v. Federal Ins. , 252 F.3d 608, 616 (2d Cir. 2001) ("the *contra proferentem* does not come into play unless this court first determines that the contract is, in fact, ambiguous.").

[119] *See* Yelitza V. Dunham, *Policyholders Continue to Secure Wins Against Liability Insurers for Defense Against IP Claims*, PRIVACY AND DATA SECURITY LAW BLOG: WINSTON & STRAWN, LLP (Apr. 4, 2019), https://www.winston.com/en/privacy-law-corner/policyholders-continue-to-secure-wins-against-liability-insurers-for-defense-against-ip-claims.html.

[120] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, §102, 116 Stat. 2322, 2323–2327 (defining various terms applicable to TRIA).

[121] Terrorism Risk Insurance Act of 2002.

[122] *See* Dan Burke, *supra*, note 107. *See also*, AMTRUST FINANCIAL, *Network Security and Privacy Liability Coverage* (Nov. 2014) (detailing all cyber insurance products offered by one of the largest insurers in the U.S.), https://amtrustfinancial.com/AmtrustFinancial/media/AFSI/PDFs/Financial%20Institutions/AFSI_Financial-Institutions_Network-Security-and-Privacy-Liability-Coverage_Summary.pdf.

[123] *See generally* Greenburg, *supra* note 52. Note, although easier to justify, certification of such attacks may also be confronted with exclusions, such as the Hostile Acts exclusions insurers have invoked in response to NotPetya. Menapace, *supra* note 114.

infrastructure systems.[124] Such a virus is inherently dangerous to human life, property, and infrastructure. However, viruses like NotPetya are highly sophisticated and require intensive cyber capabilities to develop.[125] For example, NotPetya was developed over a period of a seven years.[126] Russian hackers created NotPetya from two separately developed pieces of software – Mimikatz and EternalBlue.[127] Mimikatz was created by a French security researcher to demonstrate a vulnerability in Microsoft's operating system.[128] EternalBlue was created by the U.S. National Security Agency, "but leaked in a disastrous breach of the agency's ultrasecret files earlier in 2017."[129] Without such fortune, the cybercriminals would have been unlikely to independently create such a sophisticated virus.

2. The Necessity of U.S. Damage

The second general criterion that the attack must "have resulted in damage in the United States."[130] Damage is defined as "harmful effects on someone or something."[131] Based on the timing of enactment relative to the September 11 attacks, the framers of TRIA likely considered physical damage to U.S. lives, property, and infrastructure when legislating. However, since then, the concept of damage has expanded, especially in cyberspace. Although cyberattacks may produce physical damage,[132] most damage is not physical.[133] Cybercrime costs typically include "damage and destruction of data, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm." Some cyberattacks that produce physical damage could easily fall under the second prong of Treasury's criteria. An attack that physically damages computers in the United States,[134] or renders them

---

[124] Although, as noted above, some policies contain exclusions that reject coverage for this type of damage.

[125] *See* Greenburg, *supra* note 45 (detailing the creation of NotPetya, which was developed by combining two highly sophisticated viruses, one made by a French security researcher, and the other created by Microsoft).

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] U.S. DEPT. OF THE TREASURY, *supra* note 88, at 5.

[131] *Damages*, OXFORD LEARNER'S DICTIONARIES (2019).

[132] Simon Parker, *Understanding the Physical Damage of Cyber-Attacks*, INFOSECURITY MAG. (2017), https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/.

[133] Cybersecurity Ventures, *Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021*, 2019 Official Annual Cybercrime Report (Dec. 13, 2018) https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html.

[134] *See* Turner et. al, *supra* note 98, at 41.

completely useless,[135] would meet any definition of "damage" imagined by TRIA framers.

However, most cyberattacks against U.S. systems typically will not actually result in damage. For example, a hack may result in stolen data. But no data will be damaged. The data will be copied onto the hacker's system, but it would remain in the original system. In fact, successful hacking includes concealing or destroying evidence that the hacker is even in the system.[136] Hackers will use programs like Hacker Defender to "alter the kernel and return false information to system calls, rendering useless most tools" that detect signs of system compromise.[137] A hacker may therefore enter a system, steal data, and exit without the host knowing she was there.

Data breaches are not as geographically identifiable as physical attacks. When terrorists attacked the United States on September 11, 2001, no one questioned where the attacks occurred. However, data is stored in servers. Servers may be located in the United States, but data centers are located all over the world.[138] Due to the ease of relaying data across continents, U.S. data owned by U.S. firms is sometimes stored abroad.[139] For example, Google has nineteen data centers.[140] Eight of these centers are located either in South America, Europe, or Asia.[141] In order to safeguard data, Google "distribute[s] all data…across many computers in different locations" rather than "storing each user's data on a single machine or set of machines."[142] The data is then chunked and replicated "over multiple systems to avoid a single point of failure."[143] Google intentionally spreads data across its global network of data centers to lower the risk to any individual customer.

However, this security protocol creates difficulties for TRIP-certification purposes. Hackers who enter a network system in the United States, may, even unknowingly, steal data that is located in a data center outside of the United States. Data stolen from servers outside of the United States would not meet the standard imposed by the second Treasury criteria. If a hacker stole Google data, and caused $200 million of property and casualty damage, but some of the data was not located inside the

---

[135] *See* Greenburg, *supra* note 52.
[136] Eoghan Casey, *Investigating Sophisticated Security Breaches*, COMM. OF THE ACM Vol. 49, No. 2, 48, 49 (Feb. 2006).
[137] *Id.* at 49.
[138] *See, e.g.*, *Discover Our Data Centers*, GOOGLE DATA CENTERS (2019), https://www.google.com/about/datacenters/locations/ (listing all nineteen data center locations).
[139] *See* Roger Yu, *More U.S. Companies Push Back on Foreign Must-Store-Data-Here Rule*, USA TODAY (Aug. 12, 2017), https://www.usatoday.com/story/money/2017/08/12/more-u-s-companies-push-back-foreign-must-store-data-here-rule/558702001/.
[140] *See Discover Our Data Centers*, *supra* note 138 (listing all nineteen data center locations).
[141] *Id.*
[142] *Data and Security*, GOOGLE DATA CENTERS (2019), https://www.google.com/about/datacenters/data-security/.
[143] *Id.*

United States, the $200 million certification threshold would likely not be met. Even if a NotPetya-like virus was introduced to the Google network, causing $200 million of physical damage to Google servers, the threshold would not be met if some of that damage occurred on a server located outside of the United States.

3. Attribution

Difficulties in attribution in cyberspace may frustrate the third of Treasury's general criteria. The third criterion requires the act to "have been committed by an individual or individuals, as part of an effort to coerce the civilian population of the United States or influence the policy or affect the conduct of the United States Government by coercion."[144] This criterion has two parts. First, the attack must be committed by an individual or individuals. Second, the individual or individuals must have intended to coerce the U.S. population, influence U.S. policy, or affect U.S. Government conduct. Typically, if an attack can be attributed to a terror organization, the intent requirement may be satisfied implicitly. Terrorism, by definition, is "use of violence and intimidation, especially for political purposes."[145] Terrorists' goals are the stated intent requirement. Therefore, the government simply needs to make a determination of attribution to satisfy the third criterion.

Attribution is also necessary because of act of war exclusions. If the attack is an act of war, insurers will not be required to make payments on claims. Per typical war risk exclusion language, an act of war must be committed by "any government or sovereign power,…military, naval or air forces,… or by an agent of any such government, power, authority, or forces."[146] The attack must be "hostile" or "warlike."[147] For an attack to fall under an act of war exclusion, a governmental body or association is a necessary element.

Attribution in cyberspace for purposes of TRIP certification may prove difficult. Generally, "establishing attribution for cyber operations is difficult but not impossible."[148] Cyberspace is an open world. Any actor, from state-sponsored organizations to individuals in a basement, may commit a cyberattack. As cyberattacks usually soon met with patches to render the repeated use futile, successful cyberattacks are novel methods or viruses created for one-time use. This further creates difficulties in tracking and tracing the attack down to the original source.

But, although attribution is difficult, "[e]very kind of cyber operation – malicious or not – leaves a trail."[149] But because of the complexities involved in novel cyberattacks, according to the Federal Bureau of Investigation ("FBI"), "[n]o simple technical process or automated solution for determining responsibility for cyber operations

---

[144] *See* U.S. DEPARTMENT OF THE TREASURY, *supra* note 88, at 5.
[145] *Terrorism*, OxfordLanguages, (2019).
[146] Allyn & McNeff, *supra* note 15, at 822.
[147] *Id.* at 825.
[148] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, A GUIDE TO CYBER ATTRIBUTION, 2 (Sept. 14, 2018).
[149] *Id.*

exists."[150] So the FBI is convinced it will eventually track down the originator of any cyberattack, but "the painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability."[151] How many months it may take to attribute an attack is uncertain, as it depends on the sophistication of the virus and the attackers. For example, the WannaCry ransomware was introduced onto computer systems worldwide on May 12, 2017.[152] In December of 2017, seven months later, the United States attributed the attack to hackers backed by North Korea.[153]

As part of the 2015 reauthorization of TRIA, Congress requested Treasury conduct a study to examine and analyze "the establishment of a reasonable timeline by which the Secretary must make an accurate determination on whether to certify an act as an act of terrorism."[154] Treasury declined to delineate any kind of timeline after analyzing the possibilities.[155] Treasury suggested "the uncertainty the Secretary may face when making a responsible assessment of whether an act is an act of terrorism" requires an unknown amount of time. "An inflexible timeline for the certification process that would apply uniformly and rigidly to potentially disparate circumstances is impractical."[156] Treasury was silent on the possibility of a flexible timeline.

The speed of the certification process matters.[157] Uncertainty on whether insurers will be required to pay claims on an attack creates lags in rebuilding and stabilizing after an attack. Any delays will be "financially significant to consumers, insurers, policyholders, and taxpayers."[158] If the government requires months, as was suggested by the FBI, to attribute an attack to a terrorist organization, TRIA may fail to provide financial stability.

Due to act of war exclusions, unless a cyberattack is clearly committed by terrorists, insurers would likely attempt to deny claim payments unless absolutely required. Even after the September 11 attacks, "there was a general concern that some insurers might attempt to deny converge under existing policies by invoking the war risk exclusion."[159] This is true even though the attack was quickly attributed to al Qaeda. If an attack like the WannaCry ransomware were to be considered for TRIP certification, a seven-month window for the Secretary of the Treasury may

---

[150] *Id.*
[151] *Id.*
[152] Security Response Team, *What You Need to Know About the WannaCry Ransomware*, SYMANTEC SECURITY RESPONSE (Oct. 23, 2017), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack.
[153] Metropoulos & Platt, *supra* note 68.
[154] *See* U.S. DEPARTMENT OF THE TREASURY, *supra* note 88, at 1.
[155] *Id.* at 10.
[156] *Id.*
[157] *See id.* at 7–10.
[158] *See id.* at 10 (explaining how the decision of whether to certify an act may be financially significant, and that the length of these decisions could vary based on the facts).
[159] Allyn & McNeff, *supra* note 15, at 826.

cause major financial strife, as insurers may hold payments until attribution was made. Even after attribution is made, insurers may then attempt to apply act of war exclusions on claims. This delay is not only destructive to the financial systems that rely on TRIP but also due to certification ambiguity.

III. TRIP CERTIFICATION CRITERIA SHOULD EXPLICITLY INCLUDE CYBERTERRORISM

The unique qualities of cyberspace and cyberattacks create difficulties in certifying a cyberterrorist attack as an act of terrorism under TRIA. Congress reauthorized TRIP in 2019 without any changes. Congress should have considered these difficulties as the probability of cyberterrorists attacking U.S. targets rises. And Congress should have amended the definition of an "act of terrorism" so as to cover cyberterrorism. This amended definition would have reduce regulatory uncertainty and ensure insured parties can rely on the guarantees of TRIA.

A. Defining "Property" and "Infrastructure"

Congress should have specifically define property to include intangible property like intellectual property, data and computer software. If Congress explicitly includes intangible property as subject to TRIA coverage, the most likely cyberterrorist attacks, hacks, would be covered under TRIA. In addition, explicit inclusion of intangible property, data, and software under TRIA would enable the Secretary to apply the definition of an act of terrorism to more nuanced types of cyberattacks quickly and efficiently. Such an efficient response would quell the fears that initiated TRIA in the first place.[160] Efficiency in certification decisions is crucial for insurers and their insured. With an expanded definition of property, both insurers and insured would be better informed on their responsibilities in protecting such property and in responding to an attack.

Infrastructure should also be defined to include network infrastructure that is both tangible (hardware) and intangible (software)[161] for the same reasons Congress should have expanded the definition of property.

B. Expanding Attacks to Cyberspace

Treasury's second criterion requires the damage occurred to have resulted in the United States. The geographic requirement works well for physical attacks. However, physical components of the networks that

---

[160] *See supra* note 35 and accompanying text (noting TRIA was a response to the fears of difficulties in lending and other business decisions due to lack of terrorism risk coverage).

[161] *See* Dan Daniels, *What is Network Infrastructure?*, GIGAMON BLOG (Mar. 6, 2016), https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure/ (explaining the components of network infrastructure).

make up cyberspace are found all over the world.[162] Even data about U.S. citizens is stored all over the world.[163]

Congress should have amended the definition of an act of terrorism to reflect this expansion. Currently, the damage caused, according to TRIA, must occur within the United States, on an air carrier or vessel, or the premises of a United States mission.[164] However, as more and more attacks are located in cyberspace, TRIA should reflect the shift in location by clearly including damage that occurs against U.S. property but generally within cyberspace.

C. Streamlining Attribution

Finally, as certification decisions are complex, such decisions may require months to finalize. Attribution challenges would only add to this delay.[165] Attribution is, and will always be, a key and difficult process in cyberattacks because of the ease of anonymity in cyberspace. Congress should have attempted to expedite attribution by statutorily creating a process by which the Executive determines attribution of cyberattacks. Congress may set up a joint task force specifically for the purpose of TRIA attribution.[166] The task force would be required to determine attribution within a specified time period. At the end of the period, if no attribution is made, the Secretary, with the advice of the task force, would move or decline to certify the attack as an act of terrorism.

CONCLUSION

Under TRIA as written, the Secretary seems to have ultimate power to certify attacks as an act of terrorism. The Secretary's certification decision cannot be delegated to anyone else and cannot be challenged in court.[167] The question is not whether the Secretary can certify a cyberattack as an act of terrorism. The question is whether the Secretary will do so.

In cyberspace, events happen almost instantaneously, leading to immediate disastrous effects.[168] If the Secretary does not know whether she should certify the attack as an act of terrorism, insurers and the insured do not either. Not only does the uncertainty tie the hands of businesspeople making decisions based upon potential certifications, but the ultimate

---

[162] *Data and Security*, *supra* note 142.
[163] *See supra* text accompanying notes 142–143.
[164] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, § 102(1)(A)(iii).
[165] *See supra* text accompanying notes 149–156.
[166] Currently, many different governmental agencies independently address the issue, which lacks unity. *See, e.g.*, Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force*, U.S. DEPART. OF JUSTICE (Jul. 2, 2018); *The National Security Strategy to Secure Cyberspace*, U.S. DEPT. OF HOMELAND SEC. (Feb. 2003); *Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636*, U.S. DEPT. OF THE TREASURY (2013); *Summary: Cyber Strategy*, U.S. DEPT. OF DEF. (2018).
[167] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, § 102(1)(C); § 102(1)(D).
[168] *See, e.g.*, Greenberg, *supra* note 52.

losses fall upon the insured. Data hacking is a highly lucrative activity for cybercriminals,[169] and hacking makes up a significant portion of cybercriminal activity today.[170] Without certification, hacks claimed by terrorists that are not covered by cyber insurance will continue to fall upon the shoulders of the insured.

Congress reauthorized TRIP in 2019. To ensure consistent, efficient application of the certification process under TRIA, Congress should have augmented the Secretary's power to certify cyberattacks as acts of terrorism. Simply clarifying the Secretary's power under TRIA would have encouraged the Secretary to take steps to mitigate damages suffered by the insured. Additionally, requesting government agencies to work together to tackle attribution in cyberspace would further the goal of efficient use of TRIA. As of 2019, the Secretary has not found a need to certify any cyberattack as an act of terrorism. However, hacks in the aggregate are expected to cause $6 trillion in damages by 2021.[171] As cyberattacks become more common, the need for understanding how the Secretary may use TRIA to respond to the issue rises.

---

[169] *See supra* text accompanying notes 46–50.

[170] Charlie Osborne, *These are the Worst Hacks, Cyberattacks, and Data Breaches of 2019*, ZDNET: THE DECADE IN REVIEW (Dec. 6, 2019), https://www.zdnet.com/article/these-are-the-worst-hacks-cyberattacks-and-data-breaches-of-2019/.

[171] Morgan, *supra* note 50.