UNCLE SAM RE: IMPROVING CYBER HYGIENE AND INCREASING CONFIDENCE IN THE CYBER INSURANCE ECOSYSTEM VIA GOVERNMENT BACKSTOPPING

H. BRYAN CUNNINGHAM[*] AND SHAUHIN A. TALESH[**]

ABSTRACT

The year 2020 was a wake-up call, for the world and specifically for the cyber insurance ecosystem. The COVID-19 global pandemic reminded insurers, observers, and policymakers that actual or newly plausible attacks—including catastrophic cyberattacks—could pose existential threats to the cyber insurance ecosystem. This article examines this risk through a hypothetical catastrophic cyberattack, interviews with sixty participants across the cyber insurance ecosystem, and recent scholarly work. We find that the risk of a catastrophic cyberattack to the solvency of the global insurance ecosystem is real and that cyber insurers have not, as yet, fulfilled their promise to meaningfully improve our collective cyber hygiene. We examine several key reasons for these findings, including both a lack of data and of stability in the cyber insurance market, problems of attribution in cyberspace, and increasing uncertainty about the enforcement of war exclusions in cyber insurance coverage disputes. We offer a prioritized and

---

[*] Executive Director, Cybersecurity Research and Policy Institute, University of California, Irvine, and Cybersecurity, Privacy, and Data Protection Attorney at Zweiback, Fiset & Coleman. Former Deputy Legal Adviser to the White House National Security Council. Support for this project was generously provided by the Herman P. and Sophia Taubman Foundation, UCI Beall Applied Innovation, and the UCI Cybersecurity Policy & Research Institute. We also thank UCI law students Stephanie Lee, Hedyeh Tirgardoon, and Amruta Trivedi, and the participants across the cybersecurity insurance ecosystem who allowed us to interview them. Special thanks for their helpful review and comments to: David Coher, Principal, Strategic Planning and Power Supply, Southern California Edison; Jeffrey M. Dennis, Newmeyer & Dillion; Jen Easterly, Director, Department of Homeland Security Cybersecurity and Infrastructure Security Agency; Robert Gellman, Privacy and Information Policy Consultant; Shabnam Jalakian, Senior Vice President/Chief Information Security Officer, First American Financial; Shawn Lonergan, National Technology and Operational Resilience Leader, PwC, and Senior Advisor to United States Cyberspace Solarium Commission; Perry Taubman, Of Counsel at Ritt, Tai, Thvedt & Hodges LLP; and Andrew Walenstein, Director, Security Research and Development at BlackBerry. We look forward to incorporating this input into future versions of our evolving legislative proposal.

[**] Professor of Law, and by courtesy, Professor of Sociology and Criminology, Law & Society, University of California, Irvine.

interconnected set of proposals to shore up the cyber insurance ecosystem and incentivize needed improvements to our overall cyber hygiene. Specifically, we propose the "Catastrophic Cyberattack Resilience Act," which would create a federally-funded financial backstop for the cyber insurance ecosystem. In order to be eligible for such backstopping, insurers would be required to: comply with new data and infrastructure security and cyber incident reporting requirements; accept United States Government certifications of attribution as conclusive; and forego enforcement of war exclusions in stand-alone cyber policies. Although scholars have explored aspects of the topics covered in this article, we believe ours is the first article to rely on in-depth interviews across the cyber insurance ecosystem, to specifically incorporate key findings and recommendations of the Cyberspace Solarium Commission and recent guidance from one of the first U.S. state financial regulators to address these issues in cyber coverage, and to provide a draft legislative solution addressing these reform needs, with specific implementing language. We offer these proposals not as a "silver bullet" but as part of an urgently needed debate to spur meaningful action before—not after—the catastrophe(s) likely to come, particularly in the absence of such reforms.

TABLE OF CONTENTS

"It keeps Lloyd's of London up at night."[1]

A THOUGHT EXERCISE

Your phone buzzes in blackness and, thinking it's your alarm, you stumble into the bathroom and start a shower. Turning the faucet to steaming hot, you walk back to check your phone and realize the buzz was not an alarm but a voicemail from your daughter in college that her hot water is out and asking how she can fix it. Standard stuff.

Except when you walk back to enjoy your shower, it is spewing nothing but cold water, as is your sink, your kitchen and bathtub faucets. All cold.

Your daughter phones again to let you know the hot water in her whole apartment complex is out. It's then that you notice your phone isn't charged even though it was plugged in all night. You flip one light switch after another – nothing.

We pan back, flying out your bedroom window to reveal that your neighborhood is dark, darker than you've ever seen it. Rising up and above the houses, we see the lights of nearby neighborhoods flicker eerily, like gas lamps of centuries past. Up and up we go, seeing neighborhood after neighborhood, city after city, flicker and fade like ghosts in the night.

Then everything goes black.

It started with the water heaters. Faceless hackers found smart-home owners who left their passwords as they were when they bought the connected controllers enabling them to manage appliances from their phones, most likely "Admin" or "password". Once in, the hackers unleashed

[1] Zoom Interview with Risk Manager & Underwriter (June 25, 2019) (on file with authors).

a botnet [2]of hijacked computers to increase the energy demands of 45,000 connected water heaters, destabilizing the power grid serving the state of California.

Sound like science fiction? It's not.[3] And it gets worse.

As they hijacked your water heater, the hackers also launched a massive Distributed Denial of Service ("DDoS") attack against the infrastructure of one of Amazon Web Service ("AWS")'s designated regions, this one in the United States West. For good measure, the hackers also utilized vulnerabilities in software updating and network monitoring products to compromise numerous customer accounts hosted on the AWS West region.

As the days without hot water or electricity drag on, you continuously try to reach your insurance company for financial help in the wake of the cascading damage to your home and business, at least until your now un-rechargeable cell phone dies. Your calls will never be answered. Your insurers are broke. So are the providers of the multiple layers of re-insurance they had secured to hedge against once-in-a-century catastrophes. No one you know, and no one they know, is being paid. Families are financially ruined. Businesses of all sizes are bankrupt. Critical infrastructures of all kinds are crippled, some permanently.

Insurers quickly exhausted their bag of tricks for denying coverage – exclusions of coverage for "hostile or warlike actions", coverage limits, asserting the attack's victims misstated their cybersecurity measures when applying for coverage, and the like. Then they all went broke.

The fail-safes have failed.

---

[2] U.S. CYBERSPACE SOLARIUM COMM'N, OFFICIAL REPORT 87 (2020), https://www.solarium.gov/report [hereinafter CSC REPORT] ("'Robot networks' or botnets, are networks of computers hijacked by criminals and nation-states to promulgate their malicious activity.").

[3] See *infra* app. B for a discussion of publicly available sources relevant to the plausibility of this hypothetical.

INTRODUCTION

The year of 2020 was a wake-up call for us all, not least the global cyber insurance ecosystem.[4] Though fretted about for years, 2020 brought those who study the viability of the global insurance industry to the realization that it is possible that the world could suffer losses sufficient to wipe out the entire global reserve capital of non-life (re)insurers.

This realization coincided with the authors' study of the potential role of cyber insurers to fill the gap left by our lack (at least in the United States) of comprehensive and compulsory cybersecurity regulation. Our sixty in-depth, semi-structured interviews spanned the cyber insurance ecosystem, including actuaries, data brokers, cybersecurity and insurance lawyers, forensics experts, insurance brokers, insurance technology

[4] Although the authors initially hoped we had coined this term, the phrase "cyber insurance ecosystem" was in use at least as far back as 2016. *See The Role of Cyber Insurance In Risk Management: Hearing Before the Comm. on Homeland Sec., Subcomm. on Cybersecurity, Infrastructure Prot. and Sec. Techs.*, 114th Cong. 1 (2016) (statement of Rep. John Ratcliffe, Chairman of the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs.) [hereinafter Statement of Rep. John Ratcliffe] ("Over the next several decades, I hope to see a matured cyber insurance ecosystem that incentivizes companies of all sizes to adopt stronger cybersecurity best practices and more effective management of cyber risks against bad actors in cyber space."); Daniele Presutti, *The Ultimate Guide to Insurance Ecosystems*, ACCENTURE : BLOG (Dec. 5, 2019), https://insuranceblog.accenture.com/the-ultimate-guide-to-insurance-ecosystems (Accenture defines an "ecosystem" in connection with the insurance industry as "a network of players, from either within or outside the industry, who work together to define, build and execute market-creating customer and consumer solutions. Successful ecosystems are defined by the depth and breadth of potential collaboration among the set of players. Each party delivers an important element or capability of the consumer solution. The power of the ecosystem lies in its complementary nature. No single player needs to own or operate all components of the solution. Together, the abilities of all parties in the ecosystem are amplified, allowing the value of the ecosystem to be greater than the combined value of all of the players on their own."). For purposes of this paper, we use the term to refer to the roles of those we interviewed: actuaries, data brokers, cybersecurity and insurance lawyers, forensics experts, insurance brokers, insurance technology companies, risk managers, underwriters, and technology experts and engineers.

companies, risk managers, underwriters, and technology experts and engineers.[5]

Among other topics, we asked interviewees about: the potential for catastrophic cyberattacks and their likely impact on the cyber insurance ecosystem and United States economic and national security; the role of insurance companies as *de facto* cybersecurity regulators; the effects of constantly evolving cyber warfare on the cyber insurance ecosystem; and potential initiatives to improve our collective cyber hygiene and protect against the potential collapse of the cyber insurance ecosystem. We also studied newly emerging litigation attempting to deny coverage for cyberattacks by various war exclusions, and we reviewed cyber insurance policies containing such exclusions.

Several key findings emerged from this research and analysis:

1. There are no commonly recognized and enforceable cyber-hygiene standards, particularly in the United States.[6]
2. Cyber insurers, while theoretically positioned to fill this gap and meaningfully improve our collective cyber hygiene have not, and likely cannot under current conditions, do so.[7]
3. The cyber insurance ecosystem currently has no financial backstop (that is, no large government guarantee of financial resources to keep insurers solvent) to prevent it from being disrupted – perhaps fatally – by a catastrophic cyberattack, or series of them, or even a combination of cyberattacks and natural

---

[5] All our in-depth interviews were confidential, lasted sixty to ninety minutes, and were digitally recorded and transcribed with the consent of the interviewees. To encourage candor, we agreed not to identify any interviewee.

[6] The U.S. Government Accountability Office defines "cyber hygiene" as "a set of practices for managing the most common and pervasive cybersecurity risks." U.S. GOV'T. ACCOUNTABILITY OFF., GAO-20-241, CYBERSECURITY: DOD NEEDS TO TAKE DECISIVE ACTIONS TO IMPROVE CYBER HYGIENE 38 (2020), https://www.gao.gov/products/gao-20-241 (based on a definition developed by Carnegie Mellon University). *See* Matthew Trevors, *Cyber Hygiene: 11 Essential Practices*, CARNEGIE MELLON UNIV.: SOFTWARE ENG'G INSTIT. (Nov. 15, 2017), https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html (providing a suggested set of cyber hygiene best practices).

[7] Shauhin A. Talesh & H. Bryan Cunningham, *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. (forthcoming 2021) (manuscript 57–60) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841045).

disasters. This reality is artificially distorting the cyber insurance ecosystem.

4. In the absence of such a backstop, insurers have turned to mechanisms such as war exclusions that simultaneously cannot accomplish their intended purpose of preventing cyber insurance ecosystem collapse *and* will remain exceedingly difficult or impossible to adjudicate, leading to continuing uncertainty rather than helping to stabilize the marketplace in a rational way.
5. There appears to be a consensus that the cyber insurance ecosystem would benefit from such government financial backstopping for truly catastrophic attacks and from more universal, required cyberattack information reporting, so long as there are reasonable protections from disclosure and liability for such reporting.

Based on these findings and building on the work of the Cyberspace Solarium Commission, we propose a set of interconnected recommendations for public-private measures to both shore up the cyber insurance ecosystem in the face of potential catastrophic attacks and to improve our collective cyber hygiene and, thereby, our national and economic security. For purposes of stimulating debate, and to suggest one way these recommendations could work together, we gather the proposed measures into draft legislation: a "Catastrophic Cybersecurity Resilience Act." This proposed new law is explained in Section IV of this article and the draft legislative text itself is in Appendix A.

A number of scholars have produced extensive, high-quality analysis of many of the issues discussed in this paper, including: the likelihood, potential effects and economics of catastrophic events across the cyber insurance ecosystem; war, terrorism, and governmental action exclusions in insurance policies and related litigation; the potential role of cyber insurers as soft regulators of cybersecurity practices and improvers of our overall cyber hygiene; and potential new public-private initiatives to improve both the cyber insurance ecosystem and overall cyber hygiene, and our national and economic security.[8]

---

[8] *See, e.g.*, Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe*, 27 CONN. INS. L.J. (forthcoming 2021) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792882); Josephine Wolff, *Cyberwar By Almost Any Definition: NotPetya, the Evolution of Insurance War Exclusions, and their*

To our knowledge, however, none of these excellent prior studies have benefited from substantive interviews across the cyber insurance ecosystem, or proposed a comprehensive solution set to address three recognized gaps in this area: the paucity of publicly available information about cyberattacks and their aftermaths; effective incentives for broad and consistent improvements in cyber hygiene across businesses and economic sectors; and a strong backstopping mechanism to protect the cyber insurance ecosystem and, more broadly, our society, in the event of a truly catastrophic, ecosystem-threatening cyberattack.

We believe this is also the first work to integrate specific legislative recommendations within the framework of proposed solutions developed by the blue-ribbon United States Cyberspace Solarium Commission ("CSC"), a blue-ribbon panel created by Congress and the President in the wake of the NotPetya attacks to "answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy?" [9] The CSC issued more than eighty specific recommendations. While we do not purport to evaluate the CSC's overall work, or address specific CSC recommendations that do not directly relate to the subject of this paper, we do view the CSC report as the most

---

Application to Cyberattacks, 27 CONN. INS. L. J. (forthcoming 2021); Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy*, YALE L. J. & TECH. (forthcoming 2021) (draft available at https://ssrn.com/abstract=3746754); Shauhin A. Talesh, *How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 418 (2018); Daniel Woods & Tyler Moore, *Does Insurance Have a Future in Governing Cybersecurity?,* 18 IEEE SEC. & PRIV. 1 (2020); CSC REPORT, *supra* note 2; Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions* (Carnegie Endowment for Int'l Peace, Working Paper, 2020), https://carnegieendowment.org/files/Bateman_-_Cyber_Insurance_-_Final.pdf

[9] CSC REPORT, *supra* note 2, at 1. The CSC was an extensive, nearly eighteen-month study chaired by U.S. Senator Angus King and Representative Mike Gallagher, employing more than thirty full-time staff and hundreds of part-time senior advisors and contributing outside experts. *Id*. app. I at 151–53. In developing its findings and recommendations, the CSC conducted "200+ meetings with industry experts; 25+ meetings with academics; 50+ meetings with federal, state, and local officials; 10+ seminars/roundtables hosted by think tanks; and 20+ meetings with officials from international organizations/foreign countries." *Id*. at 21. The CSC's multiple task forces also did extensive independent research and conducted a "competitive strategy event" and external "red team" exercises by outside experts. *Id.* at 1, 21–22.

comprehensive, authoritative, and actionable recent work on the cybersecurity topics it covers.

At least twenty-five of the eighty CSC recommendations have already been enacted into United States law, with the passage in January of the most recent National Defense Authorization Act ("NDAA").[10] The most important of these is the creation of a new Senate-confirmed National Cyber Director in the White House.[11]

Several of the CSC's recommendations are directly relevant to our legislative proposal, although additional review, including consultations with experts and Congressional hearings, will be necessary to fully consider the details of these proposals. However, because of the thoroughness of the CSC's work, and the breadth of consultation that went into their proposals, we have adopted legislative language proposed by the CSC where such language is applicable and we believe it has merit, modifying it to better support the goals we outline.

In addition, we believe this is the first study and set of recommendations to suggest concrete ways to implement the February 2021 *Cyber Insurance Risk Framework* guidance by the New York Department of Financial Service ("NYDFS") specifically directed to insurers.[12] One of the first state insurance regulators to issue specific guidance on cyber insurance, NYDFS directed that "[a]ll authorized property/casualty insurers that write cyber insurance should employ the [specific] practices . . . to sustainably and effectively manage their cyber insurance risk."[13]

Although not particularly detailed, the NYDFS's key recommendations, include guidance to: "manage and eliminate exposure to

---

[10] Press Release, Angus King, U.S. Sen., *NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission* (Jan. 2, 2021), https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-commission.

[11] Maggie Miller, *Senate confirms Chris Inglis as first White House cyber czar*, HILL (June 17, 2021, 4:32 PM), https://thehill.com/policy/cybersecurity/559051-senate-unanimously-confirms-chris-inglis-as-first-white-house-cyber-czar.

[12] Colleen Theresa Brown, Thomas D. Cunningham & Sujit Raman, *New York Department of Financial Services Issues First Guidance by a U.S. Regulator Concerning Cyber Insurance*, SIDLEY AUSTIN (Feb. 10, 2021), https://datamatters.sidley.com/new-york-department-of-financial-services-issues-first-guidance-by-a-u-s-regulator-concerning-cyber-insurance.

[13] Letter from Linda A. Lacewell, Superintendent, New York State: Dept. of Fin. Servs., to All Authorized Prop./Cas. Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

silent cyber insurance risk"[14] (our proposal would only provide government financial backstopping for "stand-alone" cyber policies or policies otherwise explicitly providing cyber coverage); "educate insureds and insurance providers" [15] (we require reasonable cybersecurity measures, including training, in order to be eligible for our proposed program); and "require notice" of cyber incidents to government officials[16] (we create a national mechanism for prompt cyber incident reporting). And, of course, we intend this entire article, and each element of the resulting legislative proposal, to help reduce what NYDFS calls "systemic risk," recognizing that such risk has:

> [G]rown in part because institutions increasingly rely on third party vendors and those vendors are highly concentrated in key areas like cloud services and managed service providers. . . . Examples of such events could include a self-propagating malware, such as NotPetya, or a supply chain attack, such as the SolarWinds trojan, that infects many institutions at the same time, or a cyber event that disables a major cloud services provider.[17]

Our analysis and proposals, of course, are neither the final word nor a silver bullet on any of these topics. Other key recommendations, such as the many measures proposed by the CSC that we do not address here, will be necessary in addition to those we propose. But we hope this work will continue a vitally important conversation across government, industry, and academia and perhaps move us a few more steps down the road to a meaningful—and long overdue—reform of the cyber insurance ecosystem.

---

[14] Brown, Cunningham & Rama, *supra* note 12.

[15] *Id.*

[16] *Id.*

[17] Letter from Linda A. Lacewell, *supra* note 13. S*ee also* Abraham & Schwarcz, *supra* note 8, at 4 (explaining the difference between "silent cyber coverage," in which cyberattack claims are made against policies that "do not affirmatively provide cyber insurance in express language [but where the parties to the insurance contract] almost certainly do not intend the result and have not planned for it," and "stand-alone cyber policies," which do affirmatively cover such losses).

I. THE CYBER INSURANCE ECOSYSTEM AND THE RISKS OF CATASTROPHIC CYBERATTACK

A. KEEPING LLYOD'S UP AT NIGHT – THE RISK OF CATASTROPHIC CYBERATTACK

Standing guard above the Thames in London's financial district, the "Inside-Out" tower, with its radical architecture locating the building's elevators and other physical infrastructure outside of the building, hardly looks like the headquarters of the globe's most venerable insurance syndicate, dating to its 1688 founding at Edward Lloyd's coffee house.[18] In the midst of our hypothetical attack, the mandarins of Lloyd's are, indeed, losing sleep. This is the nightmare they have fretted over for at least the last several years.[19] Whether in the context of a massive cyberattack, pandemic, or any other context, what "keeps Lloyd's up at night," as well as many who study the cyber insurance ecosystem, is the 2020 realization that "the global non-life insurance industry's *$2 trillion in capital won't last in a 'black swan' event, such as a cyberattack* or another pandemic, that hobbles the global economy."[20]

---

[18] Julia Kagan, *Lloyd's of London*, INVESTOPEDIA (Nov. 18, 2020), https://www.investopedia.com/terms/l/lloyds-london.asp.

[19] *See, e.g.*, LLOYD'S OF LONDON, CYBER RISK: THE EMERGING CYBER THREAT TO CONTROL SYSTEMS 5 (2021), https://assets.lloyds.com/media/542bea95-0d28-4ce1-a603-63db54aa24f9/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf ("The potential for physical perils represents a major turning point for the broader cyber (re)insurance ecosystem. . . . [C]rossing the divide between information technology (IT) and operational technology (OT), along with increases in automation and the sophistication of threat actors, means it is paramount that (re)insurers carefully consider how major losses may occur and the potential impacts"); *Lloyd's targets orderly insurance market response to catastrophic events*, PINSENT MASONS LLP: OUT-LAW NEWS (July 24, 2017, 10:27 AM), https://www.pinsentmasons.com/out-law/news/lloyds-targets-orderly-insurance-market-response-to-catastrophic-events (Lloyd's of London laying out principles for an "orderly market response" to catastrophic events in 2017); LLOYD'S OF LONDON, LLOYD'S CYBER-ATTACK STRATEGY 3 (2016), https://www.lloyds.com/~/media/files/the-market/operating-at-lloyds/lloyds-cyber-attack.pdf (stating, in 2016, that cyberattacks were "the emergence of a new societal threat . . . .").

[20] Lucca de Paoli, Katherine Chiglinsky & Benjamin Robertson, *When $2 Trillion Falls Short, Next 2020 May be Uninsurable*, CLAIMS J. (Dec. 8, 2020), https://www.claimsjournal.com/news/international/2020/12/08/300867.htm (emphasis added).

The CSC starkly summarized the risk and potential consequences of a catastrophic cyberattack:

> The reality is that we are dangerously insecure in cyber[space]. Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process, and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state-sponsored intellectual property theft using cyber espionage. A major cyberattack on the nation's critical infrastructure and economic system would create chaos and lasting damage exceeding that wreaked by fires in California, floods in the Midwest, and hurricanes in the Southeast.[21]

According to one influential catastrophic loss analysis, global losses from cybercrime could reach $6 trillion in 2021.[22] In a publication entitled *When $2 Trillion Falls Short, Next 2020 May Be Uninsurable*, the insurance industry publication, "Claims Journal," stated that the "economic fallout from Covid-19 has left insurers issuing existential warnings and businesses discovering they weren't covered. It's resulted in courts packed with lawsuits and governments scrambling to head off more pain."[23] Similarly, the Cyber Risk Task Force of the American Academy of Actuaries wrote in 2020 to the U.S. Comptroller General that:

> [V]arious studies considered disruption of a cloud service provider, or a mass software vulnerability leading to widespread data breaches, or a global ransomware attack, or a cyberattack on the Northeastern U.S power grid. Economic losses associated with these events could range in

---

[21] CSC REPORT, *supra* note 2, at v.

[22] GUY CARPENTER & CO., LOOKING BEYOND THE CLOUDS 11 (2019), https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/october/Beyond-the-Clouds.pdf. *See also* Abraham & Schwarcz, *supra* note 8, at 34 (explaining the types of first and third-party losses that may arise from a cyberattack).

[23] de Paoli, Chiglinsky & Robertson, *supra* note 20.

> the hundreds of billions, and in extreme scenarios over $1 trillion.[24]

A forthcoming study entitled *Courting Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe* predicts that "$100 billion in covered losses from a cyberattack would severely wound the insurance industry, and covered losses two or three times that amount could bring the industry, or at least some of its participants, to its knees."[25] The 2020 attacks dubbed "SolarWinds"—likely still ongoing at the time of publication of this paper—will probably result in damage of at least $100 billion.[26]

As global business continued to reel from the SolarWinds attack, a likely Chinese cyberattack revealed by Microsoft in early March 2021 was "morphing into a global cybersecurity crisis, as hackers race[d] to infect as many victims as possible" before victim companies could find and defeat the

---

[24] Letter from Edmund Douglas, Chairperson, Cyber Risk Task Force, to Gene Dodaro, Comptroller Gen. of the U.S. Gov't Accountability Off. (June 1, 2020), https://www.actuary.org/sites/default/files/2020-06/GAO_Comment_Letter_TRIA_and_Cyber.pdf.

[25] Abraham & Schwarcz, *supra* note 8, at 3. Abraham and Schwarcz note, however, that, "[o]f course, not all of a future cyber catastrophe's costs will be insured. But the message of this Article is that a much larger portion of these costs would be covered than is now anticipated. In the wake of the Covid-19 pandemic, for example, insurers had to recognize the possibility—unlikely though it may have seemed a month or two earlier—that they would be responsible for a trillion dollars or more of economic losses putatively covered under Business Interruption insurance. Although insurers are ultimately unlikely to have to pay the lion's share of these losses, they could be much less fortunate in the event of a large-scale catastrophic cyber loss." *Id.* at 3–4 (internal citations omitted).

[26] Gopal Ratnam, *Cleaning up SolarWinds hack may cost as much as $100 billion*, CQ ROLL CALL (Jan. 11, 2021, 6:00 AM), https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/ (noting the so-called "SolarWinds" attacks—perhaps still ongoing as of publication of this paper—likely conducted by Russia, gained access to U.S. Government and corporate systems by compromising software-update tools sold by the company SolarWinds, thereby gaining access to compromise at least 18,000 of SolarWinds-using entities). *See also* Lucian Constantin, *SolarWinds attack explained: And why it was so hard to detect*, CSO (Dec. 15, 2020, 3:44 AM), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html (quoting a FireEye analyst's statement that the hackers used this access to "transfer files, execute files, reboot the machines, and disable system services . . . .").

threat.[27] By the time it was publicly reported, the Chinese-government-backed attack had claimed at least sixty thousand victims, including the European Banking Authority and individual banks and electricity providers, heralding another potentially nine-figure cyberattack.[28]

The risk of a catastrophic cyberattack, particularly one against a global cloud service provider, creating systemic risk across the global cyber insurance ecosystem was front-of-mind for many of our interviewees. As one risk manager stated:

> It keeps Lloyd's of London up at night. They're really, you know, they almost lost their shirt in the 70s over the Achille Lauro. And so, they do a lot of systemic risk studies these days. And they've been laser-focused on AWS because if it goes dark, right? Oh my God.[29]

B. ENABLING CATASTROPHE: WIDESPREAD WEAK CYBER HYGIENE

By any measure, cyber hygiene, both in the United States and globally, remains woefully inadequate. The United States Cybersecurity and Infrastructure Agency ("CISA") found, in January 2021, that "[d]espite the use of security tools . . . organizations typically had weak cyber hygiene practices that allowed threat actors to conduct successful attacks."[30] The CISA reports—focusing on recent attacks against cloud services—that the victims were not employing even some of the most basic cybersecurity protective techniques, such as enforcing Multifactor Authentication ("MFA") and successfully training employees against phishing attacks.[31]

A 2018 study found dismal adoption by surveyed users across most key aspects of good cyber hygiene, including password usage, response to phishing scams, sharing sensitive personal information in emails and even

---

[27] William Turton & Jordan Roberston, *Microsoft Attack Blamed on China Morphs into Global Crisis*, BLOOMBERG (Mar. 8, 2021, 3:01 AM), https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world.

[28] *Id.*

[29] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

[30] CYBERSECURITY & INFRASTRUCTURE AGENCY, U.S. DEP'T. OF HOMELAND SEC., ANALYSIS REP. NO. AR21-013A, STRENGTHENING SECURITY CONFIGURATIONS TO DEFEND AGAINST ATTACKERS TARGETING CLOUD SERVICES (2021), https://us-cert.cisa.gov/ncas/analysis-reports/ar21-013a.

[31] *Id.*

over social media, and the use of antivirus scans.[32] The authoritative CSC even argues that:

> The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide. Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing.[33]

C. LIKELY RESPONSE OF THE CYBER INSURANCE ECOSYTEM TO A CATASTROPHIC CYBERATTACK

How will the cyber insurance ecosystem respond to a multi-hundred billion or trillion-dollar catastrophe or series of catastrophes? If past is prologue, the aftermath of the September 11, 2001 terror attacks might be instructive:

> So, after 9/11 . . . the next day, you couldn't do any property placements in any major city in the United States - the market just seized. Because who's going to write [insurance policies] in New York, in Manhattan again? I mean, right? You bring whole buildings down? So, immediately TRIA [the Terrorism Risk Insurance Act] was born.[34]

Illustrating how quickly the global cyber insurance ecosystem reacts to new catastrophes, in early 2021 musicians in the United Kingdom were pushing their government to create a national "insurance fund" when insurers began refusing to cover cancelations due to the COVID-19 pandemic.[35] This follows the UK government creating such a backstopping scheme for the television and film industry.[36] For its part, the United States Congress

---

[32]Ashley A. Cain, Morgan E. Edwards & Jeremiah D. Still, *An Exploratory Study of Cyber Hygiene Behaviors and Knowledge*, 42 J. INFO. SEC. & APPLICATIONS 36 (2018).

[33] CSC REPORT, *supra* note 2, at 1.

[34] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

[35] Martin Croucher, *Musicians Join Calls for Gov't Live Music Insurance Scheme*, LAW360 UK (Mar. 1, 2021, 1:35 PM), https://www.law360.co.uk/insurance-uk/articles/1359831.

[36]*Id.*

demonstrated in 2020-2021, as it had during the economic crisis a decade earlier, that it can appropriate massive amounts of funds in short order, passing measures to spend nearly $6 *trillion* in less than a year to help the nation respond to the COVID-19 pandemic.[37]

D. CYBER INSURERS TO THE RESCUE? NOT WITHOUT HELP

Many have predicted that, in the words of one commentator, cyber insurance will "reshape cybersecurity,"[38] by collecting and analyzing large volumes of cyberattack and loss data, by prescribing and incentivizing better cyber hygiene by insureds—both by rewarding better behavior and refusing to insure, or charging higher premiums to insure, cyber hygiene laggards—and by providing pre- and post-breach cybersecurity services to their insureds. At least one congressional hearing in 2016 was devoted entirely to this expectation.[39] Based on our research, this turns out not to be the case—at least not yet.

As discussed in detail in our paper, entitled *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*,[40] we conclude that, at least as of early 2021, cybersecurity insurance providers do not seem to be systematically improving the cyber hygiene of the businesses they insure, nor are they enforcing a uniform set of best practices, procedures, technologies to ensure a robust cybersecurity posture to protect our collective national and economic security.[41] Our conclusion is reinforced by recent scholarly work coming at these problems using different methodologies.[42] As we concluded in that prior article, "insurtech interventions and innovations, while they may have benefits for the efficiency of the cyber insurance industry, are largely ineffective at enhancing organizations' cybersecurity."[43]

---

[37] Gabe Alpert, *U.S. COVID-19 Stimulus and Relief: A breakdown of the fiscal and monetary responses to the pandemic*, INVESTOPEDIA (OCT. 30, 2021), https://www.investopedia.com/government-stimulus-efforts-to-fight-the-covid-19-crisis-4799723.

[38] Asaf Lifschitz, *Cyber Insurance Will Reshape Cybersecurity*, INS. J. (Oct. 11, 2019), https://www.insurancejournal.com/news/national/2019/10/11/545228.htm.

[39] Statement of Rep. John Ratcliffe, *supra* note 4.

[40] Talesh & Cunningham, *supra* note 7.

[41] *Id.* at 59.

[42] *See, e.g.*, Bateman, *supra* note 8, at 5–11 (finding that the potential for insurers to foster improvement in overall cybersecurity remains "unrealized").

[43] Talesh & Cunningham, *supra* note 7, at 44.

Our research suggests that this failure to date is due to several factors. First, big data analysis and use in the cyber insurance ecosystem remains an unreliable tool to aid in improving the global cyber insurance ecosystem as access remains limited and available data is often not accurate or reliable.[44] Second, the data that is available appears to be used more to increase sales of insurance products than to enhance overall cyber hygiene.[45] Third, other technology tools such as security scanning and scoring by cybersecurity professionals also may not be reliable and accurate.[46] Finally, although insurers have an array of pre- and post-breach services available to their insureds, to date most insurers have not used the potential carrots (e.g., lower premiums) or sticks (e.g., denial of coverage or higher premiums) to incentivize better cyber hygiene.[47]

The findings of the CSC reinforce the views of our interviewees. In a section recognizing the potential for insurers to incentivize better cyber hygiene by businesses, noting insurers' historic role in the development of, e.g., seatbelts and airbags for automobiles and fire suppression systems in building codes, the CSC observed:

> A robust and functioning market for insurance products can have the same positive effect on the risk management behavior of firms as do regulatory interventions. Although the insurance industry plays an important role in enabling organizations to transfer a small portion of their cyber risk, it is falling short of achieving the public policy objective of driving better practices of risk management in the private sector more generally. The reasons for this failure are varied but largely come down to an inability on the part of the insurance industry to comprehensively understand and price risk, due in part to a lack of talented underwriters and claims adjusters and the absence of standards and frameworks for how cyber risk should be priced. This has had the combined effect of creating an opaque environment for enterprises attempting to purchase coverage and undermining the

---

[44] *Id.* at 44–47.

[45] *Id.* at 44, 47–54.

[46] *Id.* at 53–57.

[47] In fact, our research reveals very few buyers of cyber insurance use insurer-sponsored pre-breach services. *Id.* at 58–60.

> effectiveness of insurance as an incentive to push enterprises toward better security behavior.[48]

In sum, scholars, policymakers, and industry experts agree that, at least to date, the global cyber ecosystem remains ineffective as quasi-regulators for improving overall cyber hygiene.

II. WAR EXCLUSIONS & ATTRIBUTION PROBLEMS: KEY BARRIERS TO IMPROVED CYBER HYGIENE VIA CYBER INSURERS

Returning to the thought experiment that began this article, we deliberately did not identify our fictional attackers taking down the California power grid, though discerning readers will have a short list of likely suspects. Whoever "they" are, it is highly likely that no victims of such an onslaught—or any of their insurers—would be able to prove the identity of their direct attackers, what country or group, if any, directed them, or their true motivations for the attack. This, as discussed below, is the problem of attribution in cyberspace. This problem also can frustrate attempts by their insurers to enforce contractual defenses to paying on their claims, including the invocation of various types of "war exclusions." We take these problems in reverse order.

A. A GATHERING STORM: CYBER INSURERS' INVOCATION OF WAR EXCLUSIONS

"*Right now, the war exclusion is a huge issue. And one I think is going to… define the future of cyber insurance.*"[49]

As countless flood victims have discovered, virtually all insurance policies have "exclusions." That is, they contain clauses excluding coverage

---

[48] CSC REPORT, *supra* note 2, at 79–80. The CSC Report suggested several measures the government could take to help improve cyber insurers' positive effects on overall cyber hygiene, including: a federally funded effort to develop training and certification for insurance underwriters and claims adjusters, as well as certification frameworks for cyber insurance products; a public-private working group to help insurers pool risk models and share anonymized data; and a review of the use of war exemptions. *Id.* at 80–82. While these proposals have merit, the authors believe that the CSC proposals included in our draft law will accomplish many of the goals of these other proposals but in a more rapid and robust way.

[49] Zoom Interview with Data Aggregator (Dec. 6, 2019) (on file with authors).

if otherwise-insured damages result from specific categories of events. Such exclusions are intended, in part, to protect the solvency of the insurance companies against "correlated" cyber risks, i.e., "catastrophic loss [that] usually does not arise from a loss suffered by a single insured. . . . When correlated losses occur, they are much more likely to be catastrophic than losses resulting from uncorrelated risks."[50] The interpretation of such exclusions in cyber-related insurance policies has emerged as one of the most important potential determinants of the future shape—and perhaps even the viability—of the cyber insurance ecosystem.

Of the twenty-seven separate cyber insurance policies we analyzed, all but one had coverage exclusions for: "war"; "warlike activities"; "warlike action by military force"; "military action"; "force majeure;" "state-sponsored terrorism"; "government entity or public authority action"; and/or "acts of God."[51] Of the twenty-six policies with such exclusions, all but one included two or more of these inclusions and all of the twenty-six included an exclusion for "government entity or public authority action."[52] Though recognizing that there are important differences between several of these exclusions, for purposes of this paper, we will refer to them all collectively as "war exclusions."

Our interviews reinforced what common sense tell us: significant escalation in insurers' denials of cyberattack coverage based on war exclusions risks upending the cyber insurance ecosystem, particularly if courts either fail to decisively rule on these issues or begin routinely siding with insurers. As quoted below, one risk manager reinforced a finding from our review of cyber insurance policies, that most cyber policies contain two or more separate war exclusions, and explained the confusion and unintended consequences this situation can create.

> You have terrorism exclusions. And so you'll have carriers that will carve back cyber terrorism. But then the policy will also have a governmental acts exclusion that doesn't have any kind of carve-back. So, you're in a situation where you've got coverage for ransomware. . . . North Korea

---

[50] *See, e.g.*, Abraham & Schwarcz, *supra* note 8, at 7.

[51] These numbers are slightly higher than in some recent surveys. *See, e.g.*, *id.* at 43–44 ("According to one recent survey, approximately 75% of cyber-insurance policies sold on the admitted market exclude coverage for an 'act of terrorism, war, or military action.' Other policies simply exclude attacks committed by a 'government entity or public authority.'"(citations omitted)).

[52] Copies of the reviewed insurance policies are on file with the authors.

> launches a ransomware attack. You file your claim and it's deemed cyber terrorism. But you say, oh, this is good because I've got a cyber terrorism carve-back. Well, it's a governmental act and your governmental act exclusion doesn't have any kind of cyber terrorism carve-back. And so carriers have relied on this idea, well, that's not our intention. . . . Our intention is not to exclude a ransomware attack that's launched by North Korea. But the letter of the law and the letter of the policy states that a governmental act is excluded. And that's clearly a governmental act because we have nation-state actors. . . . Even the Chinese have state-sponsored government-paid employees that hack and launch ransomware attacks. So it just creates a lot of challenges, a lot of confusion. And I think it makes the broker's job difficult if you're not spending a whole lot of time in this."[53]

Interviewees across the cyber insurance ecosystem agreed on the possible destabilizing effects of escalating attempts to enforce war exclusions.[54]

Although eight of ten corporate leaders in a recent survey by the Economist Intelligence Unit are concerned about falling victim to a state-

---

[53] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

[54] *See, e.g.*, *id.* ("The cyber policies all have carve-backs right now for cyber terrorism. [But] if we look at the definition of terrorism, it's so broad that any grandmother that gets agitated would be considered a terrorist under a cyber policy. So, it's anybody who does any kind of malicious act for a political, religious, or ideological motive. Well, that covers every hacker I've ever run into. And so, you wouldn't have any cyber coverage unless you carved back the War on Terrorism exclusion. Right now, what we're doing because of [the denial of coverage litigation between Zurich and Mondelez] is, we're also forcing them to carve back the war exclusion for things that are—I mean, just because it's a cyber weapon doesn't mean that it was an act of war."); Zoom Interview with Ins. Broker & Ins. Tech. Entrepreneur (July 17, 2019) (on file with the authors) ("Every insurance policy, whether it's your auto policy or your homeowner policy or your D&O policy or your property policy, they all have what's called a war exclusion. That's because if there is a war there are just certain things that [are] uninsurable. . . . If you read war exclusions, they've been broadly written, and they do not work in cyber policies. For instance, they'll say, 'Any act of war, comma, hostility, comma, act of foreign government.' . . . Most people [think,] 'Oh, they'll never invoke that!'").

sponsored cyberattack,[55] until recently, war exclusions did not seem to play a significant role in cyber insurance coverage disputes. This is the case despite recognition amongst many in the cyber insurance ecosystem of the increasing prevalence and ferocity of cyberattacks appearing to be government-sponsored attacks. Our interviews consistently suggested that the "softness" of the cyber insurance market and insurer competition for market share may have accounted for this.[56]

By early 2021, however, cyber insurance market conditions appeared to be changing. An analysis by Aon suggests that cyber insurers "passed a 'tipping point' in 2020 with loss frequency and severity outpacing pricing increases and tougher underwriting."[57] The report, predicting rate hikes of between twenty and fifty percent, suggests that "ransomware events and supply-chain attacks in 2020 have prompted insurers to implement coverage changes."[58] As of March 2021, the permanence and impact of these market changes were unclear. It seems reasonable to expect, however, that increasing concerns for risk exposure in the cyber insurance ecosystem will only increase the frequency of insurers limiting coverage and attempting to enforce war exclusions and exacerbate the lack of confidence in the ability of the cyber insurance ecosystem to handle catastrophic cyberattacks.

War exclusions in cyber policies, as in previous contexts, serve a variety of purposes, but the most relevant to the instant analysis is that:

> [I]t is extremely difficult, if not impossible, to protect against State grade-attacks, so corporations cannot take, or be encouraged to take, effective defensive measures by regulators or cyber insurers. It is impossible to underwrite against a State-sponsored attack. Also, the potential scope

---

[55] Casey Johnson, *State-Sponsored Cyberattacks: A Major Threat to Businesses, Study Finds*, STREETINSIDER.COM (Feb. 22, 2021, 6:00 AM), https://www.streetinsider.com/Business+Wire/StateSponsored+Cyberattacks%3A+A+Major+Threat+to+Businesses%2C+Study+Finds/18007398.html.

[56] One cyber attorney told us: "I have no idea how these guys are underwriting this with any sense of confidence. What I am starting to get the sense from talking to these people is that the market is so saturated right now, you can get a great deal on cyber insurance." Zoom Interview with Head of Data & Prot. Prac. Grp. & Cybersecurity L. (June 5, 2019) (on file with the authors).

[57] Erin Ayers, *Cyber prices likely to rise 20% to 50% through 2021, as line reaches 'tipping point'*, ADVISEN: FRONT PAGE NEWS (Mar. 10, 2021), https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/391944676.html?rid=391944676&list_id=35.

[58] *Id.*

of a state-sponsored attack could be enormous, and potentially destabilize the cyber insurance market. [59]

B. NOTPETYA AND EARLY LITIGATION TESTS OF CYBER INSURANCE WAR EXCLUSIONS

Perhaps the closest the world has come to our hypothetical catastrophic reign of cyber terror began in June 2017 when Russia—locked in a multi-year undeclared war with Ukraine that had killed more than ten thousand Ukrainians—unleashed the most virulent malware yet seen at that point: NotPetya.[60] Disguised as ransomware, NotPetya was "honed to spread automatically, rapidly, and indiscriminately. . . . By the second you saw it, your data center was already gone."[61] The malware encrypts a victim's data in a way that cannot be undone, thus functionally obliterating all data it attacks.[62]

In February 2018, the White House publicly stated that NotPetya was a Russian government military operation, declaring that "[i]n June 2017, the Russian military launched the most destructive and costly cyber-attack in history"[63] and estimated the cost of the NotPetya attacks to be at least $10 billion.[64] One indicator of how quickly cyber threats can evolve and how related costs can escalate is illustrated in an early estimate of the cost of the 2020 "SolarWinds" hack as *ten times* that of the 2017 NotPetya attack, or north of $100 billion dollars.[65] And the damages from SolarWinds certainly

---

[59] VINCENT J. VITKOWSKY, WAR EXCLUSIONS AND CYBER THREATS FROM STATES AND STATE-SPONSORED HACKERS 10 (2017), https://insurance developments.typepad.com/files/war-exclusions-and-state hackers.pdf. See Wolff, *supra* note 8, for a history and analysis of war exclusions in the cyber insurance context.

[60] *See, e.g.*, Mike McQuade, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2010, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed -the-world/.

[61] *Id.*

[62] *Id.*

[63] Joe Uchill, *White House confirm NotPetya malware was Russian military operation*, AXIOS MEDIA: WORLD (Feb. 15, 2018), https://www.axios.com/white-house-confirms-notpetya-1518728781-ddc89bed-3b21-4d48-be5d-f2831f040b57 .html.

[64] McQuade, *supra* note 60.

[65] *What can we learn from the "most devastating" cyberattack in history?*, CBS NEWS (Aug. 22, 2018, 1:04 PM), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/.

will continue to go up. "Unlike good wine, this case continues to get worse with age," said Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. "For a lot of folks, the more they dig, the worse the picture looks."[66]

Targeted against Russia's wartime enemy, Ukraine, the 2017 NotPetya strike appears to have been aimed directly at the national and economic infrastructure of that country.[67] The weapon rapidly slipped its apparently intended bounds, however, devastating government computers in multiple countries, as well as:

> [H]ospitals in Pennsylvania . . . [and] a chocolate factory in Tasmania. It [ate into] multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, [and international food conglomerate] Mondelez. . . [And, as almost certainly not planned by its architects, NotPetya] spread back to Russia, striking the state oil company Rosneft.[68]

While the global sweep and devastating costs of NotPetya made it historic, what sent shockwaves through the cyber insurance ecosystem was the surprising response of a number of the most powerful players in that ecosystem. Despite aggressively selling cyber insurance policies for several years, NotPetya seems to have changed the calculation of at least several significant carriers. As one recent study described this evolution:

> Some property and casualty insurers declined to pay NotPetya-related claims, instead invoking their war exclusions—long-standing clauses that deny coverage for "hostile or warlike action in time of peace and war" perpetrated by states or their agents. War exclusions date

---

[66] Gopal Ratnam, *SolarWinds Hack Recovery May Cost Upward of $100B*, GOV'T TECH. (Jan. 21, 2021), https://www.govtech.com/security/SolarWinds-Hack-Recovery-May-Cost-Upward-of-100B.html.

[67] McQuade, *supra* note 60.

[68] *Id*. For a detailed summary of the NotPetya attacks, see, for example, Asaf Lubin, *Public Policy and The Insurability of Cyber Risk*, 6 J.L. & TECH. TEX. (forthcoming 2021) (manuscript at 1, 3–5, 43) (draft available at https://ssrn.com/abstract=3452833). For a discussion of NotPetya and a summary of other Russian, Chinese, and other cyberattacks against perceived enemy governments, see, for example, CSC REPORT, *supra* note 2, at 11.

> back to the 1700s, but they had never before been applied to cyber incidents.
>
> This novel use of the war exclusion, still being litigated, has raised doubts about whether adequate or reliable coverage exists for state-sponsored cyber incidents. Some observers have asked whether such incidents are insurable at all, given the potential for aggregated cyber losses even more catastrophic than those of NotPetya. [69]

In a forthcoming publication focusing on the potential effects of attempted enforcement of war exclusions, one scholar notes that: "[a]mong the most vexing issues, though, with arguably wide-ranging implications for not only the cyber risk insurance industry, but on U.S. cybersecurity policy generally, is when a cyberattack that has been attributed back to a foreign nation constitutes an act of war thus excluding coverage." [70]

When Merck & Co., Inc. ("Merck") suffered $900 million of damages at the hands of NotPetya,[71] the company was covered by numerous property insurance policies, including those issued by some of the largest insurance and reinsurance companies in the world: Allianz, Liberty Mutual, QBE, and numerous underwriting syndicates of Lloyd's, London (the "Merck Insurers").[72] According to Merck's complaint in its New Jersey state lawsuit against the Merck Insurers, the various policies sold to Merck by the Merck Insurers (the "Insurance Polices") covered "all risks of physical loss or damage to property, not otherwise excluded by the Insurance Policies, at Merck's locations worldwide."[73] More specifically, the Insurance Policies stated that "physical loss or damage shall include any destruction, distortion, or corruption of any computer data, coding, program, or software. In additional, the Insurance Policies contain a sperate insuring agreement for "Computer Systems – Non Physical Damage."[74]

Although Merck's privacy and network liability insurers covered some NotPetya losses and damages, dozens of Merck's reinsurance

---

[69] Bateman, *supra* note 8, at 1.

[70] Shackelford, *supra* note 8, at 1.

[71] McQuade, *supra* note 60.

[72] Complaint for Declaratory Relief and Compensatory Damages and Demand for Jury Trial, Merk & Co. v. Ace Am. Ins. Co., No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. Aug. 8, 2018) [hereinafter Merck Complaint] (International Indemnity Ltd. is Merck's wholly owned, so-called "captive" insurance company).

[73] *Id.* at 8.

[74] *Id.* at 8, 9.

providers denied coverage, many on the purported ground that the NotPetya attack was covered by one or more war exclusions.[75] Merck asserts, to the contrary, that "[n]o exclusion from coverage under [the Insurance Polices] —including, without limitation, any exclusion for war or terrorism" applies to the NotPetya attacks or resulting loss or damages."[76] Merck asked the New Jersey state trial court for a declaratory judgment that any exclusions for war or terrorism do not apply to exclude coverage.[77]

Similarly, pursuant to an "all risk" property insurance policy, Zurich American Insurance Company ("Zurich") denied coverage for NotPetya damages sustained by the international food giant, Mondelez, in 2016. Mondelez then filed a complaint seeking coverage for its $100 million plus NotPetya losses ("Mondelez Complaint").[78] According to the Mondelez Complaint, the Zurich policy covered "all risks of physical loss or damage," specifically to include "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction. . . ."[79]

After initially suggesting it would provide coverage,[80] Zurich informed Mondelez that it would deny coverage, based on policy Exclusion B2(a), which states:

> This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
> . . .
> 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
> (i) government or sovereign power (de jure or de facto);
> (ii) military, naval, or air force; or

---

[75] *Id.* at 11.
[76] *Id.* at 12.
[77] *Id.* at 11-16.
[78] Complaint and Jury Demand, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018-L-011008 (Ill. Cir. Ct. Oct. 10, 2018) [hereinafter Mondelez Complaint].
[79] *Id.* at 2.
[80] *Id.* at 3.

> (iii) agent or authority of any party specified in i or ii above.[81]

We use the Mondelez language for an analysis of what it might take for an insurer to prevail in these types of "war exclusion" disputes.[82]

Few have become wealthy predicting what courts will do, and it is anyone's guess whether the *Merck* or *Mondelez* courts will ever resolve the important legal issues before them and, if so, whether the two courts will agree, and the extent to which either or both rulings will withstand appeal or eventually reach beyond the two jurisdictions in which the courts sit. What is certain, however, is that the cyber insurance ecosystem is watching these cases closely. Further, a finding in favor of the reinsurers in either case will send shockwaves throughout the entire ecosystem, and could radically reshape it. As one risk manager said about the *Mondelez* litigation: "[e]verybody's sitting back and watching that one."[83]

Despite the difficulty of prediction, we can observe some clues about how a court faced with the assertion of a war exclusion in the context of a peacetime cyberattack would approach the problem.[84] By way of context, it's worth remembering the burden to demonstrate that insureds' claims fall within the relevant exclusion(s) generally falls on insurers, though this can vary depending upon the negotiating history of the policies and sophistication of the insureds or their representatives.[85] Second, as asserted in *Mondelez's* complaint, attempting to exclude coverage for a cyberattack based on a war exclusion appears to be, if not the first-of-its kind, then at

---

[81] *Id.* at 4.

[82] Based on publicly available court filings, it does not appear that either the *Merck* or *Mondelez* courts have, as of the date of publication of this article, issued any relevant dispositive orders or made any determinations of law shedding light on the issues addressed herein.

[83] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

[84] Special thanks for contributions to this analysis to University of California, Irvine Law student Hedyeh Tirgardoon and to the prior work and insightful analyses contained in Justin Ferland, *Cyber Insurance – What Coverage in Case of an Alleged Act of War? Questions Raised by the Mondelez v. Zurich Case*, 35 COMPUT. L. SEC. REV. 369 (2019). *See also* Lubin, *supra* note 68, at 43; VITKOWSKY, *supra* note 59.

[85] *See, e.g.*, Cont'l Cas. Co. v. McDowell & Colantoni, Ltd., 668 N.E.2d 59, 62 (Ill App. Ct. 1996) (as quoted in Ferland, *supra* note 84). At least in the *Mondelez* jurisdiction of Illinois, courts have held that this presumption is "especially true with respect to exclusionary clauses." Outboard Marine Corp. v. Liberty Mut. Ins. Co., 607 N.E.2d 1204, 1217 (Ill. 1992) (citing Reliance Ins. Co. v. Martin, 467 N.E.2d 287, 289–90 (Ill. App. Ct. 1984)).

least highly unusual. Third, whether articulated or not, courts likely will take into consideration the chaos upholding such an exclusion would wreak on the cyber insurance ecosystem.[86]

In the absence of clearly applicable judicial precedent applying war exclusions to cyber insurance claims, based on our review and analysis, it is likely that, in order to prevail, insurers will have to persuade courts by a preponderance of the evidence the following elements: the nature of the act; the identity and motivation of the attacker; and the context of the attack.

The first prong of the likely test for application of a war exclusion (at least under the terms of the Mondelez/Zurich policy) is whether, under the facts and circumstances of NotPetya, the attacks constituted a "hostile and warlike act." [87] Notwithstanding the use of the term in war exclusions in numerous cyber and other insurance policies, there does not appear to be a single, widely accepted definition of "hostile and warlike act."[88] Based on the few directly applicable cases, an insurer likely would have to meet at least the following three tests in order to have a realistic chance of prevailing in a war exclusion coverage dispute:

1. The Nature of the Attack

To interpret a "war" or "hostile or warlike act" exclusion,[89] courts will likely look to sources such as: the United Nations Charter, under which an "act of war" can be an "armed attack" even if the attack is not equivalent to a full-scale military assault;[90] and/or guidance promulgated by the United States Department of Defense, which defines "act of war" in the cyber context as "the direct physical injury and property damage resulting from [a] cyber event [that] looks like that which would be considered a use of force

---

[86] *See, e.g.*, Matthew C. Stephenson, *Legal Realism for Economists*, 23 J. ECON. PERSPS. 191 (2009) (discussing one of many perspectives on the role that economic considerations often play in judges' decisions).

[87] *See, e.g.*, Ferland, *supra* note 84, at 370. For illustrative purposes here, we use the exclusionary language in Mondelez's policy provided by Zurich. Obviously, the actual language of an exclusion in any particular case will significantly affect this analysis.

[88] *Id.*

[89] It seems intuitively obvious that virtually any cyberattack would be considered "hostile" by the victim of such an attack and that, therefore, the term "hostile and warlike act" must require more than just subjective hostility.

[90] VITKOWSKY, *supra* note 59, at 5.

if produced by kinetic weapons."[91] Whether or not the damages suffered by Mondelez in NotPetya reach either of these thresholds is highly debatable. Assuming, *arguendo*, that an insurance carrier could satisfy this prong, they would still have a long way to go to successfully deny coverage.

2. State of War Between Attacker and Victim

Here, it seems insurers asserting war exclusions in the NotPetya context would encounter a mixed bag of facts and circumstances. True, Russia (the presumed NotPetya attackers) had been in various stages of military conflict with the intended victim—Ukraine —for a number of years prior to NotPetya.[92] Though this was not a "declared" war, it seems unlikely that courts would consider this decisive since no wars have been formally "declared" since the mid-20th Century, at least by the United States,[93]and given the precise language of the Zurich war exclusion in *Mondelez*. It is, thus, conceivable that a court might find that a "war" existed between belligerents Russia and Ukraine in this case. Even if a court found a state of war between Russia and Ukraine, however, it is unlikely they would find that a state of war existed between Russia and the United States, such that Mondelez could be reasonably considered a target of any such war. Thus, the ground would begin to shift under cyber insurer Zurich's feet even before we get to the third prong.

---

[91] *Id.* at 6 (citing *Digital Acts of War: Evolving the Cybersecurity Conversation: Hearing Before the Subcomm. on Nat'l Sec., Subcomm. on Info. Tech., Comm. on Oversight & Gov't Reform*, 114th Cong. 1 (2016) (statement of Aaron Hughes, Deputy Assistant Secretary of Defense for Cyber Policy) ("[W]hen determining whether a cyber incident constitutes an armed attack, the U.S. Government considers a number of factors including the nature and extent of injury or death to persons and the destruction of, or damage to property."). *See also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 49.1, June 8, 1977, 1125 U.N.T.S. 3 (noting that to qualify a cyberattack as an armed attack there must be violent consequences).

[92] McQuade, *supra* note 60.

[93] Matthew Wills, *The Last Formal Declaration of War*, JSTOR: DAILY (Dec. 30, 2014), https://daily.jstor.org/the-last-formal-declarations-of-war/ ("The last time Congress formally declared war was in World War II. . . . All other wars, engagements, police actions, invasions, rescue missions, etc. since–including Korea, Vietnam, Iraq I & II, Afghanistan—have been authorized and/or funded in some way by Congress without a formal declaration of war.").

3. The Intention of the Attacker

Though no prior decision seems to be on all fours for this analysis, the most oft-cited ruling applicable to the interpretation of war exclusions in insurance policies in circumstances short of a declared war is the 1974 decision by the United States Court of Appeals for the Second Circuit in *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co*[94]. This case ruled on the applicability of war exclusions in the hijacking and destruction of a Pam Am airliner by the Popular Front for the Liberation of Palestine ("PFLP"). In that landmark decision, the court issued two holdings of potential salience here. The *Pan Am* court held that an "act of war" does not include "the inflicting of damage on the civilian property of non-belligerents by political groups, far from the site of warfare" and that "warlike operations" do *not* include:

> [1] the infliction of intentional violence by political groups (neither employed by nor representing governments) [2] upon civilian citizens of non-belligerent powers and their property [3] at places far removed from the locale or the subject of any warfare. [4] This conclusion is merely reinforced when the evident and avowed purpose of the destructive action is not coercion or conquest in any sense, but the striking of spectacular blows for propaganda effects.[95]

Granting that the NotPetya attacks do not appear intended for "propaganda effects" (except, perhaps, against the citizens of Ukraine) they almost certainly were not for the purposes of "coercion or conquest in any sense," which the *Pan Am* court appears to have found to be a *sine qua non* of a warlike action.[96]

C. THE ATTRIBUTION PROBLEM

Here we reach the heart of the matter, and one of the key rationales for our recommendations in this Section IV of this article. To meet any of these elements, an insurer would first have to persuasively "attribute" an

---

[94] Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974).

[95] *Id.* at 1015–16.

[96] *See* Abraham & Schwarcz, *supra* note 8, at 26 (noting as in any other coverage dispute, plaintiffs also would have to prove factual and proximate causation).

attack to a government or sovereign power. But proving "whodunit" in an international cyberattack, as has been widely discussed by experts on all sides of the debate, is exceedingly difficult and, often, impossible, at least without the use of highly classified government intelligence information. In addition to the intentionally distributed and anonymous nature of the internet, attackers have a myriad of tools—and lots of incentive—to disguise their identity and location. This is the ubiquitous "attribution" problem, the extreme difficulty of proving, particularly with publicly available evidence, the identity of a cyberattacker.[97]

Government officials, cybersecurity experts, and scholars across many facets of cyber warfare, defense, policy, and insurance have identified cyberattack attribution as one of the greatest challenges of the internet age.[98] As a cyber insurance data aggregator described it to us:

> [T]he real problem with the wars exclusion is that you don't know who is behind events and what the motivation was. You know, your spectrum of players range from . . . employees of . . nation states down to cyber criminals, and under different circumstances, every one of those could be combatants in cyber war.[99]

Another factor making war exclusions problematic to litigate—and adding to the uncertainty of the cyber insurance ecosystem—is that so many for-profit hacker groups also "moonlight," in support of the national security and economic objectives of their parent states, sometimes acting for profit and sometimes as agents of their governments.[100] Finally, hackers have a long history of deliberately obfuscating their origin. In so-called "false flag" attacks, a cyberattacker deliberately tries to mislead the victim and the world

---

[97] *See, e.g.*, Amir Lupovici, *The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward*, 17 INT'L. STUD. PERSPS. 322 (2016) (analyzing how cyber anonymity influences the success or failure of cyber deterrence). CSC REPORT, *supra* note 2, at 130, app. C. (defining "attribution" as the "[i]dentification of technical evidence of a cyber event and/or the assignment of responsibility for a cyber event. The technical source may be different from the responsible actor.").

[98] *See* Shackelford, *supra* note 8; *see also* CSC REPORT, *supra* note 2.

[99] Zoom Interview with Data Aggregator, *supra* note 49.

[100] *See, e.g.*, CROWDSTRIKE, 2021 GLOBAL THREAT REPORT 36, 43 (2021).

about who launched the attack and why.[101] Among recent examples of false-flag attacks in cyberspace are the 2014 North Korean attacks on Sony and the cyberattacks related to the Russo-Ukraine conflict which were orchestrated to look like they were perpetrated by Ukrainians but appear actually to have been launched by Russian intelligence.[102]

It is difficult to imagine either of the following two scenarios: first, that private civil litigants would accept as conclusive evidence, without a legal requirement to do so, a statement, even by the United States Government , that, e.g., the Government of Russia was the force behind a particular attack; or, second, that the United States Government would, again absent a legal requirement to do so, declassify for public release highly sensitive intelligence information just to resolve litigation between insurers and their insureds. Yet, it is equally unlikely that any civil litigant, on its own, will be able to introduce conclusive evidence (even by a preponderance standard) that the government of a foreign nation was behind a particular attack and prove the actual motive of such an attack.

Whether or not this is the precise analysis any court would use to interpret an exclusion for a "hostile or warlike act," by a "government or sovereign power," the key point is this: every prong of all likely tests would require information that no party to a civil court proceeding would possess. Coupled with the courts' likely awareness of how a finding for insurers on the war exclusion exemption theory would upend the cyber insurance ecosystem, it seems unlikely that either the *Mondelez* or *Merck* courts would find for the insurers.[103]

Whatever the outcome of these specific cases, the CSC and many other observers, including our interviewees, believe that the ongoing uncertainty about the outcome of these two cases – and the fear of many additional ones – continues to stand in the way of the stabilization of the cyber insurance ecosystem, and thereby enabling insurers to contribute significantly to overall improvements in cyber hygiene. Attribution problems, in turn, continue to stand in the way of making future such determinations predictable, further undermining rational cyber insurance ecosystem stabilization.

---

[101] Josh Fruhlinger, *What is a false flag? How state-based hackers cover their tracks,* CSO ONLINE (Jan. 9, 2020, 3:00 AM), https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html.

[102] *Id.*

[103] To date, neither the *Mondelez* nor *Merck* cases appear to have led to a flood of coverage denial litigation based on war exclusions. Carriers likely are awaiting the result of these cases to determine whether, and under what circumstances, to try and enforce such exclusions in future cases.

III. THE CASE FOR ACTION AND GOALS OF OUR PROPOSAL

As discussed above, many recent developments appear to be creating the conditions for a perfect storm of catastrophic cyberattack(s) sufficient to threaten the cyber insurance ecosystem. These conditions include: the inexorable and increasing pace and severity of cyberattacks; the failure of cyber insurers to step into the breach and act as effective *de facto* regulators in the absence of comprehensive government action; and the resulting failure of our collective cyber hygiene efforts.

To be sure, we may be wrong or overly alarmist about one or more of these trends. To us, though, it seems likely we will face—sooner rather than later—a cyber reckoning (or a cyber "Pearl Harbor"—pick your metaphor). More optimistically, by adequately preparing for that day, we can reduce the likelihood that it ever comes.

A. THE TIME HAS COME FOR A PUBLIC-PRIVATE CYBER INSURANCE PARTNERSHIP

Most of our interviewees who commented on the necessity of action to shore up the cyber insurance ecosystem agreed that a public-private partnership is necessary to stabilize the market and improve our overall cyber hygiene. A risk manager, for example, opined that: "[E]ventually we're going to have [a public-private solution] - as soon as we have some huge incident, people will realize that we have to do it because what'll happen is that the insurers will just quit insuring the risk."[104]

Other recent research efforts reinforce this finding. The CSC, for example, found an urgent need to raise our overall cyber hygiene levels and recognized that government would have to be part of the solution:

> Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities. Over time, this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes. In some cases, that requires aligning market forces. In other cases, where those forces

[104] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

> either are not present or do not adequately address risk, the U.S. government must explore legislation, regulation, executive action, and public- as well as private-sector investments.[105]

Abraham & Schwarz observed, in support of a government insurance backstopping program, that "[t]he social benefits of such coverage of catastrophic risk can help entire economic regions or industries to bounce-back more quickly and robustly from national catastrophes."[106]

The CSC also recognized the potential benefits of a government "backstop" such as we propose in Section IV of this article and concludes its discussion of potential strengthening the cyber insurance ecosystem by observing that:

> For the insurance industry to effectively serve as a lever to scale up risk management, the industry must mature to supply products aligned with the demands of those seeking to buy them and must increase overall premiums to take on a meaningful amount of risk. Some of this maturation will come with time, but the U.S. government is well placed to play the same role it has taken with other emerging insurance industries throughout history, facilitating collaboration to develop mature and effective risk assessment models and expertise. Cyber insurance is not a silver bullet to solve the nation's cybersecurity challenges. Indeed, a robust and functioning market for cybersecurity insurance is not an end in and of itself, but a means to improve the cybersecurity of the U.S. private sector and the security of the nation as a whole in cyberspace.[107]

---

[105] CSC REPORT, *supra* note 2, at 4. *See also, e.g.*, Lubin, *supra* note 68, at 46, 49 (noting that "[c]overage for cyber terrorism and state-sponsored attacks, offers one area where some intervention is needed for public policy reasons. The current state of the market is one of under-insurance. . . . The same logic that guided us in extending TRIA to cover losses for cyber terrorist harms, should also pave the way for offering a governmental insurance program for covering state-sponsored cyberattacks under certain extreme conditions.").

[106] Abraham & Schwarcz, *supra* note 8, at 9.

[107] CSC REPORT, *supra* note 2, at 81.

B. WHY A NEW LAW?

John Adams joked that "one useless [person] is a shame, two is a law firm, and three or more is a Congress."[108] To be sure, legislatively directed regulation can create more problems than it solves, particularly in areas in which specific technical requirements can become obsolete before the metaphorical ink on a new law dries.[109] Mindful of this, and discussed in detail herein, it is also true that a growing cadre of cybersecurity experts and academics have reluctantly concluded that only legislative and regulatory action can hope to address the risk of catastrophic cyberattack, including as it might affect the cyber insurance ecosystem.

Also potentially arguing against a legislative approach to cybersecurity has been a lack of ability or will in Congress and the executive branch, to date, to agree on a large package of measures crossing all economic sectors and the traditional opposition of powerful business interests. But this may be changing. The publication of the *CSC Report*, passage of legislation implementing its recommendations, recent hearings on—and scholarship about—the NotPetya and SolarWinds attacks, and increasing evidence that catastrophic cyberattacks on our critical infrastructure are not only technically possible, but likely being prepared and experimented with right now, is increasing a sense of urgency over the risk of catastrophic cyberattack.[110] It appears, based on early 2021 Congressional hearings, that even leaders of companies most likely to be regulated are now supportive of such regulation.[111]

---

[108] *Congress Jokes*, UP JOKES, https://upjoke.com/congress-jokes (last visited Jul. 25, 2021). *Contra Fact Check: John Adams quote about Congress stems from 1969 Broadway musical*, REUTERS (Feb. 1, 2021, 5:18 PM), https://www.reuters.com/article/uk-factcheck-john-adams-quote-congress/fact-check-john-adams-quote-about-congress-stems-from-1969-broadway-musical-idUSKBN2A13QY (noting there is some dispute as to whether the historical John Adams actually said this or only his character in the Broadway musical *1776*).

[109] *See, e.g.*, Ulrich Kühn, *Can We Still Regulate Emerging Technologies?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 09, 2019), https://carnegieendowment.org/2019/05/09/can-we-still-regulate-emerging-technologies-pub-79125 (citing the perils of government regulation of emerging technologies but concluding that it still can be done beneficially).

[110] See *infra* app. B and the CSC REPORT, *supra* note 2, for a further discussion of recent global hacker activities.

[111] *See, e.g.*, *Open Hearing on the SolarWinds Hack: Hearing Before the S. Select Comm. on Intelligence*, 117th Cong. 14 (2021) (statement of Brad Smith,

C. WHAT TO LEAVE IN, WHAT TO LEAVE OUT

It's been said the quickest way to kill any legislative proposal is to begin its title with the word "comprehensive." We don't attach the word "comprehensive" to our proposal—because it isn't. Both the CSC and recent scholarship have recommended numerous measures, beyond those we propose here, which have merit. These measures include: separate national data retention and data use laws, the creation of a joint government-private sector data-sharing center, a federal emergency funding mechanism akin to those under the Stafford Act for natural disasters (possibly triggered by a "Cyber State of Distress" declaration),[112] the creation of a national Bureau of Cyber Statistics and various iterations of government, public-private, or decentralized attribution mechanisms.[113]

Our approach prioritizes what our research suggests are the most urgent problems facing the cyber insurance ecosystem to create an interconnected set of measures we believe can work to maximize our collective ability to prevent, mitigate, and recover from the type of catastrophic cyberattack that befell our hapless fictional water heater owners. We also tried to balance the need for government involvement with concerns about heavy-handed, mandatory legal regulations. We fear that such heavy regulation would be too inflexible for the ever-changing cyber threat environment and cyber insurance ecosystem market conditions, and as a result, likely would face likely insurmountable opposition in a closely divided Congress.

We do not intend this cluster of proposals to be *the* solution—as is often noted, there are no silver bullets here. Although we believe the

---

President, Microsoft Corp.) ("A private sector disclosure obligation will foster greater visibility, which can in turn strengthen a national coordination strategy with the private sector which can increase responsiveness and agility. The government is in a unique position to facilitate a more comprehensive view and appropriate exchange of indicators of comprise and material facts about an incident."); *Open Hearing on the SolarWinds Hack: Hearing Before the S. Select Comm. on Intelligence*, 117th Cong. 14 (2021) (statement of Kevin Mandia, CEO, FireEye Inc.).

[112] *CSC Report*, *supra* note 2, at 4–5, 103–04 (recommendations 4.7, 5.2.2, 5.2, and 3.3, respectively).

[113] *See, e.g.*, *id.*; Adam Bobrow, *Quantifying Risk: Innovative Approaches to Cybersecurity*, THE GERMAN MARSHALL FUND OF THE U.S. 2 (Apr. 28, 2021), https://www.gmfus.org/publications/quantifying-risk-innovative-approaches-cybersecurity; Shackelford, *supra* note 8, at 43–44; Abraham & Schwarcz, *supra* note 8.

measures we selected are complementary, could be effectively integrated, and are not "comprehensive" enough to be doomed, the measures we include in our proposal could be decoupled and/or combined with other laws or executive actions. And we hope they will serve as a departure point for a vigorous debate around potentially viable solutions and, most importantly, persuade lawmakers and cyber insurance ecosystem participants alike that, collectively, we must do *something.*

And that the clock is running. A recent study by the Carnegie Endowment for International Peace concluded that " [i]n the wake of a major cyber disaster, there would be louder calls for a formal cyber backstop. [Although] [i]t would be smarter and cheaper to create one in advance."[114]

Inviting slings and arrows, then, we present, in Appendix A, the "Catastrophic Cyberattack Resilience Act" ("CCRA"), a proposed law we hope suggests how a set of measures could be enacted and work together.[115] We intend the CCRA to be a starting point for debate, but one based on real-world data gathered via our interviews, review of prior scholarship, analysis of cyber insurance policies and recent cyber denial-of-coverage litigation, and what we believe to be some of the most authoritative and helpful recent work on the cyber insurance ecosystem, including that of the CSC, the NYDFS, and the scholars cited herein.

---

[114] Bateman, *supra* note 8, at 52.

[115] The CSC Report defines "resilience" as "the capacity to withstand and quickly recover from attacks that could compel, deter, or otherwise shape U.S. behavior . . ." and finds resilience to be "a foundational element of layered cyber deterrence, ensuring that critical functions and the full extent of U.S. power remain available in peacetime and are preserved in crisis." CSC Report, *supra* note 2, at 54. In urging a number of the specific measures we propose, the CSC stressed the importance of national resilience. The CSC's proposed strategy "calls for denying benefits to adversaries by promoting national resilience, reshaping the cyber ecosystem, and advancing the government's relationship with the private sector to establish an enhanced level of common situational awareness and joint collaboration. The United States needs a whole-of-nation approach to secure its interests and institutions in cyberspace." *Id.* at 4.

D. OBJECTIVES OF THE CATASTROPHIC CYBERATTACK RESILIENCE ACT

Title I of the CCRA would establish the "Catastrophic Cyberattack Insurance Program" ("Program"), a federally funded financial "backstop" for insurers in the wake of truly catastrophic cyberattacks. Based on, but not identical to, the Terrorism Risk Insurance Act ("TRIA"), we intend the measure to help protect the solvency of the cyber insurance ecosystem, to reduce market uncertainties persisting in the absence of such protection, and to better enable the cyber insurance ecosystem to fulfill its promise of improving overall cyber hygiene. This is the measure's primary objective.

In addition, we view the draft CCRA as an opportunity to kick-start several other key mechanisms to stabilize the cyber insurance ecosystem and improve our overall cyber hygiene. We would do this by offering the carrot of participation in the backstop funding (and/or the stick of losing the availability of such funds) and by creating institutional mechanisms to help develop standards and procedures to manage these efforts. Importantly though, no requirement in the CCRA is a mandatory legal or regulatory obligation. The requirements are only enforceable on those insurers who choose to participate in the Program.

Under CCRA, in order be eligible for the new federal Program, an insurer must:

- Mandate that all purchasers of the insurer's cyber products maintain a baseline level of cyber hygiene, as determined jointly by the Secretary of the Treasury, the CISA, and the new National Cyber Director (recently created by Congress based on the CSC's recommendations) ("NCD");
- Require all insureds to make timely reporting of cyber incidents, coupled with mandatory, but protected, information sharing and requirements for the government to make the gathered information public to the greatest extent consistent with disclosure limitations and national security concerns;
- Abide by (and not challenge in litigation) newly created public "certifications of attribution" for cyberattacks, to be issued by the Secretary of the Treasury, in consultation with CISA and the NCD. These determinations would be supported by the national Cyber Threat Intelligence Integration Center (the

codification of which we adopt as proposed by the CSC); and

- Agree, in most circumstances, to not enforce war exclusions in cyberattack coverage decisions or litigation.[116]

In addition, the backstopping funds would only apply to losses covered by stand-alone cyber policies or other policies explicitly including cyber coverage. In this way, we hope also to meaningfully reduce "silent cyber" risks.

By coupling government insurance backstopping for catastrophic cyberattacks with a set of requirements to qualify for such backstopping, we believe the government can nudge the cyber insurance ecosystem towards its promise of improving overall cyber hygiene without overly specific, heavy-handed government regulation. No insurer would be *required* to impose new CCRA mandates on their insureds and no insured would be *required* to buy coverage with the CCRA requirements. But given the concerns we found across cyber insurance ecosystem participants, we believe it likely that many participants in that ecosystem would adopt the "best practices" measures in the CCRA in return for stabilization of the market, increased access to cyberattack information, significant reduction or elimination of war exclusion litigation and "silent cyber" risks, and protection from liability for cyberattack information sharing.

IV. THE CATASTROPHIC CYBERATTACK RESILIENCE ACT

A. THE ANATOMY OF THE CCRA

1. TITLE I – The Comprehensive Cyberattack Insurance Program

This section of our proposed CCRA was adapted from the current, compiled version of TRIA. With this approach, we intend to take advantage of the nearly twenty years of legislative reconsiderations and modifications to the original TRIA. We recognize, of course, that the final appropriate

[116] *See infra* app. A Titles II–V. While we have fashioned our proposals as a draft bill for consideration in the United States Congress, state legislatures and/or state insurance regulators could consider elements of the CCRA for adoption in their jurisdictions. It seems unlikely, however, that any individual state in the United States could provide the financial backstopping we propose.

legislative language for a program like CCRA likely will differ in other ways from the language we adapted from TRIA. Additional fact-finding and analysis would be required to determine precisely what further deletions, additions, and changes may be required to adapt the successful mechanisms of TRIA to the cyber insurance ecosystem.

Much like TRIA operates, CCRA would give the Secretary of the Treasury (the "Secretary") the authority, in consultation with CISA and the NCD, to trigger CCRA backstopping by certifying the incident as a catastrophic cyberattack. To be so certified, a cyberattack would have to have losses from cyber risk coverage exceeding, or reasonably expected to exceed, $10 billion.[117] Also like TRIA, certifications under CCRA would be final and unreviewable.

We have made several important, provisional judgments in Title I which should be analyzed by scholars and experts in this area, including through Congressional hearings considering any such proposal. Highlighting the most consequential of these:

(a) Damage Threshold for Certification, Initial Federal Funding, and Elimination of Upper Limit.—Our recommended initial threshold of $10 billion in insured losses is admittedly somewhat arbitrary and suffers from the same lack of available data plaguing the entire cyber insurance ecosystem. We propose this threshold for debate as consistent both with expected damages from cyberattacks and the level of loss payouts reasonably likely to cripple or destroy cyber insurers.[118] Moreover, just as our understanding of the risk and economics of large terrorist attacks has evolved, leading to changes in the TRIA thresholds, we would expect the threshold in any final version of the CCRA, and future amendments to it, to evolve with experience and data.

As drafted, Title I would provide up to $50 billion in initial funding for federal payments under the Program. This number undoubtedly would change— perhaps dramatically—through deliberations of an actual CCRA and, candidly, represents what intelligence officers call a "WAG" (Wild-

---

[117] Our proposal, as drafted, contemplates circumstances in which the Secretary, in consultation with the new National Cyber Director and the Cybersecurity Infrastructure and Security Agency, can certify an attack if the amounts may be "reasonably" expected to meet the required damage and insured loss thresholds. *See infra* app. A Title I §102 (1)(A). We believe this ability would allow federal "reinsurance" for attacks that do not appear to meet the thresholds at the time of certification but, much like the 2020 SolarWinds-related attacks, are likely to end up being exponentially more costly than initially apparent. This also would allow a timely federal response in cases where the damages will accumulate over time.

[118] *See* discussion *supra* Section 1.

Assed Guess). Compared to most TRIA projections, it is a spectacularly high number. As discussed above, though, compared to potential comprehensive cyberattack losses, it is a modest one and, in the event of a truly catastrophic cyberattack, additional appropriations obviously would be necessary, but Congress has made plain throughout the COVID-19 pandemic its capacity for rapidly spending far more than this amount.

As an initial amount, however, we feel that $50 billion could accomplish two equally important goals. First, it should be sufficient to jump start payments to insurers in the immediate wake of a catastrophic cyberattack, staving off potential collapse. Second, and at least as important, it would provide the cyber insurance ecosystem with much-needed confidence in the long-term cyber insurance market.

We also eliminated TRIA's upper limit for certification because we believe that imposing any upper limit would weaken the ability of the CCRA to stabilize the cyber insurance ecosystem. Further, if the CCRA reinsurance provisions are ever triggered, this likely would require a new Congressional appropriation and those future legislators, guided by state insurance regulators and other experts, would be better positioned to determine, based on economic conditions at the time and the other national and economic security and societal effects of the catastrophic cyberattack, whether an upper limit, if any, should be imposed.

(b) Limitation to damage "within the United States."—This will serve as a limiting principle for CCRA and to focus potentially huge amounts of United States taxpayer dollars on improved cyber hygiene and the cyber ecosystem in the United States. Although the original TRIA also extended coverage to United States' facilities overseas and United States' aircraft and vessels, we did not include this provision in the draft CCRA.

(c) Removal of all provisions for recoupment of federal funds spent under the Program and required deductibles to be applied to participating insurers.—This choice likely will be controversial and may threaten, in the minds of some, the entire financial viability of the CCRA. Nonetheless, we decided not to include these provisions in our initial proposal for two reasons.

First, given the massively higher damage amounts contemplated by CCRA, it seems unlikely that many insurers would be able to meet any significant deductible percentage. Also, as discussed above, Congress and the executive branch at the time of a future catastrophic cyberattack would

be better positioned to determine, based on conditions at the time whether any recoupment requirements would be justified, feasible, and wise.[119]

2. TITLE II – Data and Infrastructure Security Requirements for Participation in the Catastrophic Cyberattack Insurance Program

Title II of CCRA would leverage access to the federal backstopping funds in Title I as an incentive to insurers to impose upon their insureds reasonable data and infrastructure security requirements, with the goal of improving our overall cyber hygiene and national and economic security. The current draft legislative text is taken largely from the CSC's legislative proposal 4.7: "Pass a National Data Security and Privacy Protection Law."[120]

Title II would establish the first national, cross-economic-sector data and infrastructure security requirement in United States history. Although there are an infinite potential combinations of such standards, we adapted Title II from the CSC legislative recommendation and legislative proposal 4.7 both because of the thoroughness and breadth of expertise involved in the CSC process and because we think it strikes a good balance between understandability and enforceability without being overly prescriptive.

In Title II, we made significant alterations to the original CSC proposal which should be analyzed by interested scholars and experts:

(a) Addition of "information technology infrastructure" security.—We added this as a requirement under Title II because we feel the protection of critical infrastructure beyond data is important, particularly when trying to protect against catastrophic cyberattack. Also, we feel that many of the specific measures contemplated by the CSC proposal would improve the protection of cyber-related infrastructure as well as data.

(b) Focus on data and infrastructure security without data retention, destruction, and use requirements.—CSC's legislative proposal also included data retention and destruction standards and data use regulations. We elected not to include these in our proposal. We believe that data retention and destruction standards, and data use protections are critically

---

[119] See *infra* app. A Title I §101 for the CCRA's draft Congressional findings and purpose language ordinarily generated after hearings and other legislative fact finding. The CCRRA's draft findings reflect our research and interviews but almost certainly would be modified and enhanced through the legislative process.

[120] U.S. CYBERSPACE SOLARIUM COMM'N, LEGISLATIVE PROPOSALS 141 (2020), https://www.solarium.gov/report [hereinafter LEGISLATIVE PROPOSALS].

important [121] (particularly from a privacy and civil liberties protection standpoint) and would strongly support national legislative action in this area. However, we do not believe these provisions have been sufficiently studied or debated. Similarly, we do not see a sufficient national consensus or agreement among the many interested parties to include these protections in this draft CCRA.

3. TITLE III – National Cyber Incident Reporting for Catastrophic Cyberattack Insurance Program Participation

CCRA's Title III likewise would use the "carrot" of federal backstopping funds to incentivize insurers to impose upon their insureds reasonable cyber incident requirements. Our research, and recent Congressional testimony by business leaders, has persuaded us not only that such a requirement is long overdue and might for the first time have the support of key industry players, but also that it could, over time, create data sets and analysis to enable the cyber insurance ecosystem to better understand, price, and manage cyber risk, with the goal of improving our overall cyber hygiene and national and economic security. The legislative language in the CCRA draft is taken largely from the CSC's legislative proposal 5.2.2: "Pass a National Cyber Incident Reporting Law."[122]

As drafted by the CSC, and modified by the authors, the CCRA's legislative proposal requires notification to include at least the following elements:

> (1) The date, time, and time zone when the cybersecurity incident began, if known.
> (2) The date, time, and time zone when the cybersecurity incident was detected.
> (3) The date, time, and duration of the cybersecurity incident.
> (4) The circumstances of the cybersecurity incident, including the specific critical infrastructure systems or subsystems believed to have been accessed or damaged and the information acquired, if any, and any

[121] One of the authors has worked extensively on data retention and destruction standards and data use protection issues over the past two decades.

[122] LEGISLATIVE PROPOSALS, *supra* note 120, at 220–23.

> information reasonably believed to be relevant for certifying attribution of the cybersecurity incident.
> (5) Any information reasonably believed to be relevant for certifying attribution of the required under this Act.
> (6) Any planned and implemented technical measures to respond to and recover from the incident.
> (7) In the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.[123]

The major changes we made to the CSC draft were to add the attribution language in requirement (4) and to eliminate the sections creating an elaborate process for identifying "mandatory reporting" entities.[124] Because CCRA applies to all entities insured by participating insurers, we did not feel the "mandatory reporting" provisions were necessary. If, however, legislators wanted to narrow the scope of the notification requirements, these provisions might provide a helpful mechanism for doing so.

4. TITLE IV – Acceptance of Cyberattack Attribution Certification for Catastrophic Cyberattack Insurance Program Participation

The CCRA's new provision (drafted by the authors) requires, as a condition of participation in CCRA's backstopping, that insureds agree to abide by, and not attempt to litigate, any "Certificate of Attribution" publicly issued by the Secretary (in consultation with CISA and the NCD). The Secretary *must*, within no more than ninety days after a catastrophic cyberattack resulting in damage within the United States, publicly certify the identity of the attackers responsible for the attack and whether they acted on behalf of a foreign nation. If the Secretary determines, within the ninety days, that such an identification is not possible with reasonable certainty, the Secretary must publicly certify this.

For non-catastrophic cyberattacks, the Secretary *may* still issue a public certification of attribution. The CCRA would make the Secretary's

---

[123] *Infra* app. A Title III §303(B); *see also* LEGISLATIVE PROPOSALS, *supra* note 120, at 222.

[124] *See infra* app. A Title III; *see also* LEGISLATIVE PROPOSALS, *supra* note 120, at 223.

determinations final and not subject to judicial review and provides for the protection of intelligence sources and methods in any public certification.

To support the Secretary's new responsibility, this draft provision would, based on the CSC's recommendation and legislative proposal 1.4.1, "Codify and Strengthen the Cyber Threat Intelligence Integration Center."[125] Under CCRA, this newly statutory center would provide staffing, expertise, analysis, drafting, and declassification review support for the attribution certification process.

The CCRA also makes certifications of attribution final and non-reviewable. CRRA's Title I, Section 106, covering litigation management, requires "[a]ny Certification of Attribution of a catastrophic cyberattack published under this Act shall be conclusive in any action under this Act, and shall not be subject to review."[126]

5. TITLE V – Non-Assertion of War Exclusions for Catastrophic Cyberattack Insurance Program Participation

As currently drafted, Title V of the CCRA requires that, in order to participate in the CCRA backstopping, an insurer "shall not seek to enforce any War Exclusion . . . in connection with a cyberattack to deny or limit coverage or payment to an insured of an otherwise valid claim."[127] Relatedly, in Title I of the CCRA, war exclusions are declared invalid and unenforceable.

We believe this provision has the potential both to enhance certainty in the cyber insurance ecosystem and to lead, eventually, to insurers determining more effective ways to limit their potential liability without eviscerating coverage insureds reasonably believe they have or leading to more bespoke negotiations by sophisticated and powerful insureds to deal with war exclusions that, as discussed above, do not really work in the cyber insurance context.

In addition to addressing this issue substantively in Title V of the CCRA, as with the certification of attribution deference discussed above, in Title I, Section 106 of the CCRA, dealing with litigation management, we specify that: "No War Exclusion shall have any force or effect in any litigation subject to this Act."[128]

---

[125] LEGISLATIVE PROPOSALS, *supra* note 120, at 27.
[126] *Infra* app. A Title I §106(a)(3)(A).
[127] *Infra* app. A Title V §501.
[128] *Infra* app. A Title I §106(a)(3)(B).

B. THE PROPOSED CCRA: POSSIBLE CRITIQUES AND ALTERNATIVES

1. Cost

We recognize that the threshold amounts, potential governmental financial responsibility, and even the initial $50 billion appropriation, are eye-popping. We are open to alternatives, of course, and invite the debate. In addition to the reasons suggested above, we believe that these amounts are matched (or perhaps even too low) to the magnitude of risk and the need to stabilize the cyber insurance ecosystem. It is also possible, of course, particularly if the Program succeeds in incentivizing better cyber hygiene, that the government funds will never be spent.

2. Lack of Upper Limit of Government Financial Responsibility, Recoupment Mechanism, or Deductibles for Insurers

We address this concern above and there may well be some ways to improve the proposal in this area, such as requiring surcharges on cyber insurance policies to help fund the initial appropriation and giving the Secretary more authority to require recoupment if financial conditions after a catastrophic attack warrant.

3. Providing Direct Catastrophic Cyberattack Emergency Funds or Loans Following an Attack

These options have been discussed by Abraham and Schwarcz and other commentators[129] and the creation of direct emergency funds also was suggested by the CSC.[130] Such options may be helpful, either as alternatives or in addition to our proposal. We are skeptical that they alone would be sufficient, however, as we do not believe they would incentivize the cyber insurance ecosystem to help enhance overall cyber hygiene.

---

[129] *See* Abraham & Schwarcz, *supra* note 8, at 54–62.
[130] CSC REPORT, *supra* note 2.

4. Risks of, and Alternatives to, Binding Government Attribution Certifications

Some commentators disfavor binding attribution certifications by governments, citing concerns that elected officials may act with "political" or other motives other than being as truthful and accurate as possible in public pronouncements.[131] Others challenge such a solution as being overly restrictive on civil litigants. These are valid potential concerns and should be debated. On the other hand, all litigants and many non-governmental commentators also will have strong and self-serving interests not necessarily consistent with impartial truth finding. Also, at least in the United States, the government likely will be in the best position—with access to classified intelligence, other information, and related analytical expertise—and it has strong motivations to provide truthful public assessments, including protecting United States taxpayer dollars by not making reckless or ill-motivated public attribution statements.[132] There have been several alternative proposals to address the vexing problem of cyberattack attribution, including by the Atlantic Council and Microsoft, favoring more multilateral and public/private attribution mechanisms.[133]

5. Belt and Suspenders – and Suspenders

Careful readers and legislative language mavens will notice a number of cases in which our proposal includes multiple provisions intended to perform the same legislative work. For example, we include, in CRRA's Section 103(b), a prohibition on the Secretary making payments to an insurer unless the insurer has "required all insureds to meet or exceed all requirements of Titles II-V of this Act as a mandatory condition for being issued an insurance policy,"[134] but we also, in those following titles, make compliance a condition for participation in the Catastrophic Cyberattack Resilience Program. We also build redundancy into other sections, including CCRA's Section 102 (definitions) and 106 (litigation management).

In any final legislation, one option likely would be selected. Where we have multiple provisions performing the same legislative work in this initial draft proposal, we intend both to reinforce the goal for any reviewer

---

[131] Lubin, *supra* note 68, at 47 (one of the authors of this article shares this concern).

[132] *Id.* at 46 n.203.

[133] *Id.* at 46 n.207.

[134] *See infra* app. A Title I §103(b)(2).

of the language and to suggest that there are multiple approaches possible to achieve the same objective. Similarly, one could reasonably argue that if war exclusions are made unenforceable, there is reduced need for a governmental certification of attribution or, conversely, that if such certifications of attribution are conclusive in litigation, this mitigates the negative effects of insurers seeking to enforce war exclusions. While we believe it helpful to include both provisions, it may be that further debate and legislative fact finding would conclude that one approach is both sufficient and preferable to the other.[135]

C. WHY NOT TRIA?

1. The Terrorism Risk Insurance Act

The United States Government has created a successful catastrophic event insurance backstop before to protect insurers from prohibitively high risk. Coverage for acts of terrorism was routinely provided at no additional charge in most general insurance policies prior to the attacks of September 11, 2001.[136] Immediately following the attacks, however, coverage for such acts became impossible to obtain or prohibitively expensive.[137]

In response to this potentially existential threat to the commercial property and casualty insurance ecosystem at the time,[138] Congress created TRIA, first signed into law in 2002. [139] Initially created as a temporary program, TRIA achieved its intended results of stabilizing the insurance market and reinstating terrorism coverage and it has been reauthorized four times, most recently in 2019.[140] The mechanism for achieving this success is

---

[135] Experienced drafters and analysts of legislation likely will also find technical drafting errors and formatting mistakes or inconsistencies. Obviously, these would need to be identified and corrected during the hearing and markup process, if not before.

[136] BAIRD WEBEL, CONG. RSCH. SERV., R45707, TERRORISM RISK INSURANCE: OVERVIEW AND ISSUE ANALYSIS FOR THE 116TH CONGRESS I (2019), https://crsreports.congress.gov/product/pdf/R/R45707.

[137] *Id.*

[138] The September 11, 2001 attacks have been estimated to have cost the insurance industry $47 billion. *Terrorism Risk Insurance Act (TRIA),* NAT'L ASSOC. OF INS. COMM'RS (Oct. 18, 2021), https://content.naic.org/cipr_topics/topic_terrorism_risk_insurance_act_tria.htm.

[139] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002).

[140] *Terrorism Risk Insurance Act (TRIA)*, *supra* note 138.

a federal program enabling the United States Government to share with insurers the risk of catastrophic losses due to terrorist attacks.[141]

For any terrorist attack above a certain, periodically adjusted, financial loss threshold, TRIA provides that federal funds will assist insurers by providing federal reimbursement for significant portions of the losses absorbed by insurers. Generally speaking, the greater the magnitude of financial loss from an attack, the greater proportion of the payouts to insureds are backstopped by the federal government.[142]

More specifically, when any act of terror (in the United States or to its air carriers or sea vessels) generating more than $5 million in losses is certified by the Secretary, in consultation with the Attorney General and Secretary of Homeland Security, the government shares the losses with insurers where "'the aggregate industry insured losses resulting from such certified acts of terrorism' exceed $180 million (increasing to $200 million in 2020)."[143] In order to qualify for such funding however, insurers must make terrorism insurance available to commercial policyholders and reveal both the premium charged for such insurance and possible federal contributions.[144] While policy purchasers are not required to buy terrorism coverage, insurers may exclude losses from acts of terror if the customer elects not to do so.[145]

TRIA also requires the government to recoup 140% of government outlays under the program through future surcharges on relevant policies.[146] Although, thankfully, the financial thresholds to activate TRIA have never been triggered, the program has been a success, as evidenced by the fact that successive congresses and presidents have reauthorized the program four times over the past twenty years, most recently at the end of 2019.[147] In fact, the non-partisan Congressional Budget Office estimates that TRIA will actually reduce the federal budget deficit by $1.4 billion.[148]

TRIA's innovative nature, and apparent success over nearly two decades, naturally begs the question of why some legislative tweaks to TRIA could not be used to address at least some of the issues we address in our

---

[141] *Id.*

[142] *See* Lubin, *supra* note 68, at 44 n.193.

[143] WEBEL, *supra* note 136, at 4.

[144] *Id.* at 6.

[145] *Id.*

[146] *Id.* at 4.

[147] *Terrorism Risk Insurance Act (TRIA)*, *supra* note 138.

[148] Perry Beider & David Torregrosa, *Federal Reinsurance for Terrorism Risk and Its Effects on the Budget* 1 (Cong. Budget Off., Working Paper No. 2020-04, 2020), https://www.cbo.gov/system/files/2020-06/56420-CBO-TRIA.pdf.

draft CCRA. In fact, as discussed below, the Department of the Treasury acted several years ago to try and clarify the extent to which cyber *terror* attacks might qualify for TRIA protection. Potentially amending TRIA is not an unreasonable option to consider, and the 2019 TRIA reauthorization legislation directed the government to study and report on amending the law to "meet the next generation of cyber threats."[149] We believe this is not the best option.

2. TRIA Cannot Sufficiently Backstop the Cyber Insurance Ecosytem or Incentivize Better Cyber Hygiene

We see multiple reasons why TRIA—even as clarified by December 2016 Treasury Department guidance that stand-alone cyber-insurance policies can qualify for TRIA protection[150]—does not provide the kind of backstop against a truly catastrophic cyberattack that most agree is needed. As outlined in a June 1, 2020 letter from the American Academy of Actuaries, these impediments include: the fact that a significant amount of cyber coverage is included in *non*-stand-alone insurance policies, including professional liability coverage, which are specifically excluded from TRIA; and uncertainty across the cyber insurance ecosystem as how changes to National Association of Insurance Commissioners ("NAIC") insurance policy coding could affect potential TRIA protections.[151]

In addition, it would be legislatively awkward to try and add our cyber hygiene-related provisions to TRIA but then only apply them to protection against catastrophic cyber incidents. The much higher catastrophe thresholds we believe are appropriate for a catastrophic cyberattack insurance program also do not seem appropriate for traditional TRIA protections. Moreover, for the reasons previously discussed,[152] we do not believe the deductible and recoupment mechanisms integral to TRIA are appropriate in the catastrophic cyber context.

Most importantly, however, the payout of any TRIA funds requires a public finding by the Secretary that an event was caused by *non-*

---

[149] Further Consolidated Appropriations Act, 2020, Pub. L. No. 116–94, 133 Stat. 2534, 3027 (2019).

[150] Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 Fed. Reg. 95312, 95312–13 (Dec. 27, 2016).

[151] Letter from Edmund Douglas, *supra* note 24, at 2–3.

[152] *See* discussion *supra* Section IV.A.1.

governmental terrorists.[153] This requirement would embroil any attempt to use TRIA to backstop losses from a catastrophic cyberattack in all of the attribution difficulties discussed above.[154] Finally, it is precisely the type of foreign government-sponsored cyberattacks excluded from TRIA protections that are the most likely to trigger a cyber insurance ecosystem-threatening catastrophe like the hypothetical one in our thought exercise.

CONCLUSION

Of the many lessons of 2020, one of the most important for the global cyber insurance ecosystem is that catastrophic losses, potentially of a magnitude to threaten the stability, or even existence, of cyber insurance, may well be possible. Among the reasons such a catastrophe appears increasingly plausible is the poor state of cyber hygiene among a significant percentage of insured businesses. Cyber insurers have yet to fulfill early expectations that they could use their relationships with, and ability to incentivize, their insureds towards greatly improved cybersecurity practices and procedures.

With the dual goals of stabilizing the cyber insurance ecosystem and improving overall cyber hygiene, we propose a series of interconnected measures to provide a United States Government funded financial backstop to keep cyber insurance carriers solvent in the event of a catastrophic cyberattack. We also look to incentivize insurers, in return for such government protection, to require their insureds to comply with new data and infrastructure security and cyber breach notification requirements, refrain from enforcing war exclusions in cyber insurance policies, and accept newly-mandated government certifications of attribution for cyberattacks.

Building on the work of the blue-ribbon CSC and data from our sixty in-depth interviews across the cyber insurance ecosystem, we present, in Appendix A, a draft CCRA. We present this proposed new law not as an end to debate but as a vehicle to further, with a sense of urgency, a much-needed translation of scholarship and recommendations into action.

---

[153] Letter from Edmund Douglas, *supra* note 24, at 3.
[154] *Id.*

APPENDIX A: THE CATASTROPHIC CYBERSECURITY RESILIENCE ACT[155]

A BILL

To ensure the continued financial capacity of insurers to provide coverage for risks from cyberattack, to incentivize stronger cyber hygiene, to require cyberattack incident disclosures and information sharing, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS

(a) SHORT TITLE.—This Act may be cited as the "Catastrophic Cyberattack Resilience Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

[155] Title I of this draft legislation is based, in significant part, though not always taken verbatim from, the Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, Title I, 116 Stat. 2322 (current version at Terrorism Risk Insurance Program Reauthorization Act of 2019, Pub. L. No 116-94, 133 Stat. 2534 (2019)). TRIA has been amended four times. The full, current text of the law is available on the Department of the Treasury website at *Statutes, Regulations, and Interim Guidance*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program/statutes-regulations-and-interim-guidance (last visited Aug. 29, 2021). Titles II, III, and IV were adapted from legislative proposals drafted by the CSC, though the authors have modified and added to them significantly. *See* LEGISLATIVE PROPOSALS, *supra* note 120. Title V was drafted by the authors.

TITLE I—CATASTROPHIC CYBERINSURANCE RISK INSURANCE PROGRAM

SEC. 101. CONGRESSIONAL FINDINGS AND PURPOSE.

(a) FINDINGS.—The Congress finds that—

(1) the ability of businesses and individuals to obtain insurance at reasonable and predictable prices, in order to spread the risk of both routine and catastrophic loss, is critical to economic growth and the stability and solvency of vital economic sectors in the United States and, in an interconnected world, globally;

(2) providers of cyber insurance are important financial institutions, the products of which allow mutualization of risk and the efficient use of financial resources and enhance the ability of the economy to maintain stability, while responding to a variety of economic, political, environmental, and other risks with a minimum of disruption;

(3) the ability of the insurance industry to cover the unprecedented financial risks presented by potential catastrophic cyberattacks in the United States can be a major factor in recovering from such attacks while maintaining the stability of the economy;

(4) widespread financial market uncertainties, including the absence of information from which insurers can make statistically valid estimates of the probability and cost of future catastrophic cyberattacks, frustrate insurers' ability to reasonably assess the size, funding, and allocation of the risk of loss caused by future catastrophic cyberattacks;

(5) decisions by cyber insurers to deal with such uncertainties, either by terminating coverage for losses arising from catastrophic cyberattacks, by radically escalating premiums to compensate for risks of loss that are not readily predictable, or through the use of war exclusions or other traditional methods to limit insurer risk, could cripple critical infrastructure and other sectors of the economy and otherwise suppress economic activity;

(6) the United States Government should provide a significant financial backstopping program for cyber insurers in the event of a future catastrophic cyberattack, contributing to the stabilization of the United States economy in a time of national crisis; and

(7) incentivized by this financial backstopping, cyber insurers can meaningfully enhance cyber hygiene across many vital sectors of our economy by mandating reasonable data and infrastructure security measures by their insureds, and cyber incident notification and information sharing by their insureds.

(b) PURPOSE.—The purpose of this Title is to establish a federal program that provides a mechanism for preserving the financial stability of the cyber insurance industry in the event of a catastrophic cyberattack on the United States, in order to—

(1) increase stability in the cyber insurance market and give confidence to providers of cyber insurance to deliver better, and more rationally priced and limited, cyber insurance products to entities across the United States economy;

(2) incentivize stronger cyber hygiene, and require cyberattack incident disclosures and information sharing; and

(3) reduce the use of policy exclusions by insurers to block or minimize coverage for damages caused by cyberattacks that are ineffective in the cyberattack context and create certainty in coverage disputes through certifications of attribution.

SEC. 102. DEFINITIONS.

(a) DEFINITIONS.—In this Act, the following definitions shall apply:

(1) CATASTROPHIC CYBERATTACK.—

(A) CERTIFICATION.—The term 'catastrophic cyberattack' means any act that is certified by th e Secretary, in consultation with the National Cyber Director and the Cybersecurity Infrastructure and Security Agency —

(i) to be a cyberattack;

(ii) to have resulted in damage within the United States; and

(iii) at the time of certification has caused, or is reasonably likely to cause, aggregate uninsured losses in excess of $10 billion;

(B) LIMITATION.—No act shall be certified by the Secretary as a catastrophic cyberattack if the act is committed as part of the course of a war declared by the Congress, except that this clause shall not apply with respect to any coverage for workers' compensation.

(C) DETERMINATIONS FINAL.—Any certification of, or determination not to certify, an act as a catastrophic cyberattack under this Act shall be final and shall not be subject to judicial review.

(D) TIMING OF CERTIFICATION.—Not later than nine months after the effective date of this Act, the Secretary shall issue final

rules governing the process by which the Secretary shall certify whether an act is a catastrophic cyberattack under this Title.

(E) NONDELEGATION.—The Secretary may not delegate or designate to any other officer, employee, or person, any determination under this paragraph of whether, during the effective period of the Program, a catastrophic cyberattack has occurred.

(2) AFFILIATE.—The term 'affiliate' means, with respect to an insurer, any entity that controls, is controlled by, or is under common control with, the insurer

(3) ATTRIBUTION.—The term 'attribution' means the identification of technical evidence of a cyberattack and/or the assignment of responsibility for a cyberattack.[156]

(4) CYBER RISK INSURANCE.—The term 'cyber risk insurance' means insurance products covering risks arising from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks, as well as physical damage that can be caused by cyberattacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information.[157] This term includes both "stand-alone" cyber risk insurance policies and other insurance policies explicitly including cyber risk coverage. This term does not include insurance policies not explicitly addressing cyber risk (so-called "silent" cyber risk coverage).

(A) the term 'cyber risk insurance' does not include any of the following types of insurance unless such insurance explicitly includes cyber insurance coverage as part of, or an endorsement to, the policy—

---

[156] Adapted from CSC REPORT, *supra* note 2, at 130.

[157] This definition is from the U.S Department of the Treasury's 2016 guidance concerning "how insurance recently classified as 'Cyber Liability' for purposes of reporting premiums and losses to state insurance regulations will be treated under TRIA and Treasury's regulations for the Program (Program Regulations)." Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 Fed. Reg. at 95312.

(i) Federal crop insurance issued or reinsured under the Federal Crop Insurance Act (7 U.S.C. 1501 et seq.), or any other type of crop or livestock insurance that is privately issued or reinsured;

(ii) private mortgage insurance (as that term is defined in section 2 of the Homeowners Protection Act of 1998 (12 U.S.C. 4901)) or Title insurance;

(iii) financial guaranty insurance issued by monoline financial guaranty insurance corporations;

(iv) insurance for medical malpractice;

(v) health or life insurance, including group life insurance;

(vi) flood insurance provided under the National Flood Insurance Act of 1968 (42 U.S.C. 4001 et seq.);

(vii) reinsurance or retrocessional reinsurance;

(viii) commercial automobile insurance;

(ix) burglary and theft insurance;

(x) surety insurance;

(xi) professional liability insurance;

(xii) farm owners multiple peril insurance; or

(xiii) property or casualty insurance.

(5) INFORMATION TECHNOLOGY INFRASTRUCTURE.—The term ‘information technology infrastructure’ shall include all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

(6) INSURED LOSS.—The term 'insured loss' means any loss resulting from a catastrophic cyberattack (including an act of war, in the case of workers' compensation) that is covered by primary or excess cyber risk insurance issued by an insurer if such loss occurs within the United States.

(7) INSURER.—The term 'insurer' means any entity, including any affiliate thereof—

(A) that is—

(i) licensed or admitted to engage in the business of providing primary or excess insurance in any State;

(ii) not licensed or admitted as described in clause (i), if it is an eligible surplus line carrier listed on the Quarterly Listing of Alien Insurers of the NAIC, or any successor thereto;

(iii) approved for the purpose of offering cyber insurance by a federal agency in connection with maritime, energy, or aviation activity;

(iv) a State residual market insurance entity or State workers' compensation fund; or

(B) that receives direct earned premiums for any type of commercial cyber risk insurance coverage; and

(C) that meets any other criteria the Secretary may reasonably prescribe.

(8) NAIC.—The term 'NAIC' means the National Association of Insurance Commissioners.

(9) PERSON.—The term 'person' means any individual, business or nonprofit entity (including those organized in the form of a partnership, limited liability company, corporation, or association), trust or estate, or a State or political subdivision of a State or other governmental unit.

(10) PROGRAM.—The term 'Program' means the Catastrophic Cyberattack Insurance Program established by this Title.

(11) SECRETARY.—The term 'Secretary' means the Secretary of the Treasury.

(12) STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, each of the United States Virgin Islands, and any territory or possession of the United States.

(13) UNITED STATES.—The term 'United States' means the several States, and includes the territorial sea and the continental shelf of the United States, as those terms are defined in the Violent Crime Control and Law Enforcement Act of 1994 (18 U.S.C. 2280, 2281).

(14) WAR EXCLUSION.—The term ‘war exclusion’ means an exclusion of coverage in an insurance policy for: “war;” “warlike activities;” “warlike action by military force;” “military action;” “force majeure;” “state-sponsored terrorism;” “government entity or public authority action;” “acts of God’” or any other exclusionary language the purpose or intent of which is to exclude insurance coverage for any type of armed conflict or other governmental action, as reasonably determined by the Secretary in regulations.

(15) RULE OF CONSTRUCTION FOR DATES.—With respect to any reference to a date in this Title, such day shall be construed—

(A) to begin at 12:01 a.m. on that date; and

(B) to end at midnight on that date.

SEC. 103. CATASROPHIC CYBERATTACK INSURANCE PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—

(1) In general.—There is established in the Department of the Treasury the Catastrophic Cyber Insurance Program.

(2) Authority of the Secretary.—Notwithstanding any other provision of State or Federal law, the Secretary shall administer the Program, and shall pay the Federal share of compensation for covered insured losses.

(b) CONDITIONS FOR FEDERAL PAYMENTS.—No payment may be made by the Secretary under this section with respect to an insured loss that is covered by an insurer, unless—

(1) the person that suffers the insured loss, or a person acting on behalf of that person, files a claim with the insurer;

(2) the insurer had required all insureds to meet or exceed all requirements of Titles II-V of this Act as a mandatory condition for being issued an insurance policy;

(3) the insurer processes the claim for the insured loss in accordance with appropriate business practices, and any reasonable procedures that the Secretary may prescribe; and

(4) the insurer submits to the Secretary, in accordance with such reasonable procedures as the Secretary may establish—

(A) a claim for payment of the Federal share of compensation for insured losses under the Program;

(B) written certification—

(i) of the underlying claim; and

(ii) of all payments made for insured losses; and

(iii) of its compliance with the provisions of this Act.

(B) PROGRAM TRIGGER.—In the case of a certified catastrophic cyberattack, no compensation shall be paid by the Secretary under subsection (a), unless the aggregate industry insured losses resulting from such a certified cyberattack exceeds, or is reasonably expected to exceed, $10 billion.

(C) PROHIBITION ON DUPLICATIVE COMPENSATION.—The Federal share of compensation for insured losses under the Program shall be reduced by the amount of compensation provided by the Federal Government to any person under any other Federal program for those insured losses.

(3) NOTICE TO CONGRESS.—The Secretary shall notify the Congress if estimated or actual aggregate insured losses are expected to exceed $100 billion during any calendar year. The Secretary shall provide an initial notice to Congress not later than fifteen days after the date of a catastrophic cyberattack, stating whether the Secretary estimates that aggregate insured losses will exceed $10 billion.

(4) FINAL NETTING.—The Secretary shall have sole discretion to determine the time at which claims relating to any insured loss or catastrophic cyberattack shall become final.

(5) DETERMINATIONS FINAL.—Any determination of the Secretary under this Act shall be final, unless otherwise expressly provided, and shall not be subject to judicial review.

SEC. 104. GENERAL AUTHORITY AND ADMINISTRATION OF CLAIMS.

(a) GENERAL AUTHORITY.—The Secretary shall have the powers and authorities necessary to carry out the Program, including authority—

(1) to investigate and audit all claims under the Program; and

(2) to prescribe regulations and procedures to effectively administer and implement the Program, and to ensure that all insurers and self-insured entities that participate in the Program are treated comparably under the Program.

(b) INTERIM RULES AND PROCEDURES.—The Secretary may issue interim final rules or procedures specifying the manner in which—

(1) insurers may file and certify claims under the Program;

(c) CONSULTATION.—The Secretary shall consult with the NAIC, as the Secretary determines appropriate, concerning the Program.

(d) CONTRACTS FOR SERVICES.—The Secretary may employ persons or contract for services as may be necessary to implement the Program.

(e) CIVIL PENALTIES.—

(1) IN GENERAL.—The Secretary may assess a civil monetary penalty in an amount not exceeding the amount under paragraph (2) against any insurer that the Secretary determines, on the record after opportunity for a hearing—

(A) has intentionally provided to the Secretary erroneous information regarding premium or loss amounts;

(B) has intentionally failed to comply with all requirements of this Act or intentionally provided to the Secretary erroneous information regarding compliance with such requirements;

(C) submits to the Secretary fraudulent claims under the Program for insured losses; or

(D) has otherwise failed to comply with the provisions of, or the regulations issued under, this Act.

(2) AMOUNT.—The amount under this paragraph is no less than $250,000 and no greater than $5 million per act in violation of this

Act, as reasonably determined by, and announced in, public regulations promulgated by the Secretary pursuant to this Act.

(f) FUNDING.—

(1) FEDERAL PAYMENTS.—There are hereby appropriated, such sums as may be necessary but not to exceed $50 billion without additional appropriations, to make initial payments of the Federal share of compensation for insured losses under the Program in the immediate aftermath of a catastrophic cyberattack.

(2) ADMINISTRATIVE EXPENSES.—There are hereby appropriated, out of funds in the Treasury not otherwise appropriated, such sums as may be necessary to pay reasonable costs of administering the Program.

(g) REPORTING OF CYBERSECURITY INSURANCE DATA.—

(1) AUTHORITY.—During the calendar year beginning on January 1, 2023, and in each calendar year thereafter, the Secretary shall require insurers participating in the Program to submit to the Secretary such information regarding insurance coverage for cybersecurity losses as the Secretary considers appropriate to analyze the effectiveness of the Program, which shall include information regarding—

(A) lines of insurance with exposure to such losses;

(B) premiums earned on such coverage;

(C) geographical location of exposures;

(D) pricing of such coverage;

(E) the take-up rate for such coverage;

(F) the amount of private reinsurance for catastrophic cyberattacks purchased;

(G) an analysis of the overall effectiveness of the Program;

(H) an evaluation of any changes or trends in the data collected under this paragraph;

(I) an evaluation of whether any aspects of the Program have the effect of discouraging or impeding insurers from providing cyberattack coverage;

(J) an evaluation of the impact of the Program on workers' compensation insurers; and

(K) such other matters as the Secretary considers appropriate.

(3) PROTECTION OF DATA.—To the extent consistent with the provisions of this Act, the Secretary shall contract with an insurance statistical aggregator to collect the information described in this Act, which shall keep any nonpublic information confidential and provide it to the Secretary in an aggregate form or in such other form or manner that does not permit identification of the insurer submitting such information.

(4) ADVANCE COORDINATION.—Before collecting any data or information under paragraph (1) from an insurer, or affiliate of an insurer, the Secretary shall coordinate with the appropriate State insurance regulatory authorities and any relevant government agency or publicly available sources to determine if the information to be collected is available from, and may be obtained in a timely manner by, individually or collectively, such entities. If the Secretary determines that such data or information is available, and may be obtained in a timely matter, from such entities, the Secretary shall obtain the data or information from such entities. If the Secretary determines that such data or information is not so available, the Secretary may collect such data or information from an insurer and affiliates.

(5) CONFIDENTIALITY.—

(A) RETENTION OF PRIVILEGE.—The submission of any non-publicly available data and information to the Secretary and the sharing of any non-publicly available data with or by the Secretary among other Federal agencies, the State insurance regulatory authorities, or any other entities under this Act shall not constitute a waiver of, or otherwise affect, any privilege arising under Federal or State law (including the rules of any Federal or State court) to which the data or information is otherwise subject.

(B) CONTINUED APPLICATION OF PRIOR CONFIDENTIALITY AGREEMENTS.—Any requirement under Federal or State law to the extent otherwise applicable, or any requirement pursuant to a written agreement in effect between the original source of any

non-publicly available data or information and the source of such data or information to the Secretary, regarding the privacy or confidentiality of any data or information provided to the Secretary, shall continue to apply to such data or information after the data or information has been provided pursuant to this Title.

(C) INFORMATION-SHARING AGREEMENT.—Any data or information obtained by the Secretary under this Title may be made available to State insurance regulatory authorities, individually or collectively through an information-sharing agreement that—

(i) shall comply with applicable Federal law; and

(ii) shall not constitute a waiver of, or otherwise affect, any privilege under Federal or State law (including any privilege referred to in subparagraph (A) and the rules of any Federal or State court) to which the data or information is otherwise subject.

(D) AGENCY DISCLOSURE REQUIREMENTS.—Section 552 of Title 5, United States Code, including any exceptions thereunder, shall apply to any data or information submitted under this Title to the Secretary by an insurer or affiliate of an insurer.

(E) PUBLIC AVAILABILITY OF INFORMATION AND REPORTS.—To the extent consistent with the other provisions of this Title, the Secretary shall make information collected pursuant to this Title publicly available.

SEC. 105. PRESERVATION PROVISIONS.

(a) STATE LAW.—Nothing in this Act shall affect the jurisdiction or regulatory authority of the insurance commissioner (or any agency or office performing like functions) of any State over any insurer or other person—

(1) except as specifically provided in this Act; and

(2) except that—

(A) the definition of the term 'catastrophic cyberattack' in section 102 shall be the exclusive definition of that term for purposes of compensation for insured losses under this Act, and shall preempt any provision of State law that is inconsistent with that definition, to the extent that such provision of law would otherwise apply to any type of insurance covered by this Title;

(B) during the period beginning on the date of enactment of this Act and for so long as the Program is in effect, as provided in section 108, including authority in subsection 108(b), books and records of any insurer that are relevant to the Program shall be provided, or caused to be provided, to the Secretary, upon request by the Secretary, notwithstanding any provision of the laws of any State prohibiting or limiting such access.

(b) EXISTING REINSURANCE AGREEMENTS.—Nothing in this Title shall be construed to alter, amend, or expand the terms of coverage under any reinsurance agreement in effect on the date of enactment of this Act. The terms and conditions of such an agreement shall be determined by the language of that agreement.

SEC. 106. LITIGATION MANAGEMENT.

(a) PROCEDURES AND DAMAGES.—

(1) IN GENERAL.—If the Secretary makes a determination pursuant to section 103 that a catastrophic cyberattack has occurred, there shall exist a Federal cause of action for property damage, personal injury, or death arising out of or resulting from such catastrophic cyberattack, which shall be the exclusive cause of action and remedy for claims for property damage, personal injury, or death arising out of or relating to such act of catastrophic cyberattack, except as provided in subsection (b).

(2) PREEMPTION OF STATE ACTIONS.—All State causes of action of any kind for property damage, personal injury, or death arising out of or resulting from a catastrophic cyberattack that are otherwise available under State law are hereby preempted, except as provided in subsection (b).

(3) SUBSTANTIVE LAW.—The substantive law for decision in any such action described in paragraph (1) shall be derived from the law, including choice of law principles, of the State in which such

catastrophic cyberattack occurred, unless such law is otherwise inconsistent with or preempted by Federal law, except that—

(A) Any Certification of Attribution of a catastrophic cyberattack published under this Act shall be conclusive in any action under this Act, and shall not be subject to review; and

(B) No War Exclusion shall have any force or effect in any litigation subject to this Act.

(4) JURISDICTION.—For each determination described in paragraph (1), no later than ninety days after the occurrence of a catastrophic cyberattack, the Judicial Panel on Multidistrict Litigation shall designate 1 district court or, if necessary, multiple district courts of the United States that shall have original and exclusive jurisdiction over all actions for any claim (including any claim for loss of property, personal injury, or death) relating to or arising out of a catastrophic cyberattack subject to this Act. The Judicial Panel on Multidistrict Litigation shall select and assign the district court or courts based on the convenience of the parties and the just and efficient conduct of the proceedings. For purposes of personal jurisdiction, the district court or courts designated by the Judicial Panel on Multidistrict Litigation shall be deemed to sit in all judicial districts in the United States.

(5) PUNITIVE DAMAGES.—Any amounts awarded in an action under paragraph (1) that are attributable to punitive damages shall not count as insured losses for purposes of this Title.

(6) AUTHORITY OF THE SECRETARY.—Procedures and requirements established by the Secretary under section 50.82 of part 50 of Title 31 of the Code of Federal Regulations (as in effect on the date of issuance of that section in final form) shall apply to any cause of action described in paragraph (1) of this subsection.

(b) EXCLUSION.—Nothing in this Act shall in any way limit the liability of any government, an organization, or person who knowingly participates in, conspires to commit, aids and abets, or commits any cyberattack with respect to which a determination described in subsection (a)(1) was made.

(c) RIGHT OF SUBROGATION.—The United States shall have the right of subrogation with respect to any payment or claim paid by the United States under this Title.

(d) EFFECTIVE PERIOD.—This section shall apply only to actions described in subsection (a)(1) that arise out of or result from certified catastrophic cyberattacks that occur or occurred during the effective period of the Program.

SEC. 107. TERMINATION OF PROGRAM.

(a) TERMINATION OF PROGRAM.—The Program shall terminate on December 31, 2035

(b) CONTINUING AUTHORITY TO PAY OR ADJUST COMPENSATION.—Following the termination of the Program, the Secretary may take such actions as may be necessary to ensure payment for insured losses arising out of a catastrophic cyberattack occurring during the period in which the Program was in effect under this Title, in accordance with the provisions of section 103 and regulations promulgated thereunder.

(c) REPEAL; SAVINGS CLAUSE.—This Title is repealed on the final termination date of the Program under subsection (a), except that such repeal shall not be construed—

(1) to prevent the Secretary from taking, or causing to be taken, such actions under subsection (b) of this section, paragraph (4), (5), (6), (7), or (8) of section 103(e), or subsection (a)(1), (c), (d), or (e) of section 104, as in effect on the day before the date of such repeal, or applicable regulations promulgated thereunder, during any period in which the authority of the Secretary under subsection (b) of this section is in effect; or

(2) to prevent the availability of funding under section 104(g) during any period in which the authority of the Secretary under subsection (b) of this section is in effect.

TITLE II—DATA AND INFORMATION TECHNOLOGY INFRASTRUCTURE SECURITY REQUIREMENTS FOR PARTICIPATION IN CATASTROPHIC CYBERATTACK INSURANCE PROGRAM

SEC. 201. DATA AND INFORMATION TECHNOLOGY INFRASTRUCTURE SECURITY.

(a) IN GENERAL.—In order to be eligible for participation in the Catastrophic Cyberattack Insurance Program, an insurer shall:

(1) establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect the confidentiality, integrity, availability, security, and accessibility of data in its possession or control, and to protect its information technology infrastructure from disabling attack; and

(2) require all purchases of cyber insurance to meet the requirements of this Title.

(b) DATA AND INFORMATION TECHNOLOGY INFRASTRUCTURE SECURITY REQUIREMENTS.—The data and information technology infrastructure security policies and practices required under subsection (a) shall be, at a minimum—

(1) appropriate to the size and complexity of the particular entity, the nature and scope of the covered entity's collection or processing of individual data, the nature and volume of the individual data at issue, and the nature, complexity, and criticality of the entity's information technology infrastructure; and

(2) designed to—

(A) identify and assess reasonably foreseeable human or technical risks or vulnerabilities to data, including unauthorized access, access rights, and use of service providers, and to protect its information technology infrastructure from disabling attack;

(B) take preventative and corrective action to address anticipated and known risks or vulnerabilities to data and to protect its information technology infrastructure from disabling attack, which may include implementing administrative, technical, or physical safeguards or changes to data security policies or practices; and

(C) receive and respond to unsolicited reports of vulnerabilities by entities and individuals.

(c) TRAINING.—The data and information technology infrastructure security policies required under subsection (a) shall provide for training all employees on how to safeguard individual data and protect individual privacy and to protect the information technology infrastructure, including updating that training as necessary; and training for all employees designing or procuring such systems.

(d) RULEMAKING.—

(1) IN GENERAL.—The Secretary may, pursuant to a proceeding in accordance with section 553 of Title 5, United State Code, issue regulations to identify processes for receiving and assessing information under this Act.

(2) CONSULTATION WITH THE CYBERSECURITY INFRASTRUCTURE AND SECURITY AGENCY, THE NATIONAL CYBER DIRECTOR, AND NIST.—In promulgating regulations under this subsection, the Secretary shall consult with, and take into consideration guidance from, the Cybersecurity Infrastructure and Security Agency, the National Cyber Director and the National Institute of Standards and Technology.

(e) GUIDANCE.—Not later than one year after the date of enactment of this Act, the Secretary shall issue guidance to covered entities on how to—

(1) identify and assess vulnerabilities to individual data and to information technology infrastructure, including—

(A) the potential for unauthorized access to data or disabling attacks on information technology infrastructure;

(B) human or technical risks or vulnerabilities to data and information technology infrastructure; and

(C) the management of access rights; and

(2) take preventative and corrective action to address risks and vulnerabilities to individual data and information technology infrastructure; and

(3) provide effective data and information technology infrastructure security and privacy training as described in subsection (c).

(f) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS.—An insured that is required to comply with Title V of the Gramm-Leach-Bliley Act (15 U.S.C 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of Title XI of the Social Security Act (42 U.S.C. 6801 et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note), and is in compliance with the information security requirements of such regulations, part, Title, or Act (as applicable), shall be deemed to be in compliance with the 152 requirements of this section with respect to data subject to requirements of such regulations, part, Title, or Act.

TITLE III—NATIONAL CYBER INCIDENT REPORTING[158] FOR PARTICIPATION IN CATASTROPHIC CYBERATTACK INSURANCE PROGRAM

SEC. 301. In order to be eligible for participation in the Catastrophic Cyberattack Insurance Program, an insurer shall report any cyber incident of itself, and require such reporting of its insureds, as required in this Title.

SEC. 302. CRITERIA AND PROCEDURES. The Secretary, in consultation with the National Cyber Director and the Cybersecurity Infrastructure and Security Agency, shall establish and publish—

(a) criteria for the types and thresholds of cyber incidents to be reported under this Title; and

(b) procedures to comply with reporting requirements pursuant to this Title.

---

[158] Based upon CSC's Legislative Proposal 5.2.2 ("Pass a National Cyber Incident Reporting Law"), as modified by authors. *See* LEGISLATIVE PROPOSALS, *supra* note 120, at 220–23.

SEC. 303. CYBERSECURITY INCIDENT REPORTING REQUIREMENTS.

(a) IN GENERAL.—An insurer, in order to be eligible for the Program, will meet the requirements of this paragraph if, upon becoming aware of the possibility that a cybersecurity incident, including an incident involving ransomware, social engineering, malware, unauthorized access, or damage or disruption to information technology infrastructure, the insurer—

(1) promptly assesses whether or not such an incident occurred, and submits a notification meeting the requirements of subsection (b) to the Secretary through the reporting processes established by the Secretary, in consultation with the National Cyber Director and the Cybersecurity Infrastructure and Security Agency as soon as practicable (but in no case later than seventy-two hours after the entity first becomes aware of the possibility that the incident occurred);

(2) provides all appropriate updates to any notification submitted under paragraph (1); and

(3) requires its insureds to comply with all provisions of this Title.

(b) CONTENTS OF NOTIFICATION.—Each notification submitted under subparagraph (b) of paragraph (1) shall contain the following information with respect to any cybersecurity incident covered by the notification:

(1) The date, time, and time zone when the cybersecurity incident began, if known.

(2) The date, time, and time zone when the cybersecurity incident was detected.

(3) The date, time, and duration of the cybersecurity incident.

(4) The circumstances of the cybersecurity incident, including the specific information technology infrastructure systems or subsystems believed to have been accessed and information acquired, if any.

(5) Any information reasonably believed to be relevant for certifying attribution of the cybersecurity incident as required under this Act.

(6) Any planned and implemented technical measures to respond to and recover from the incident.

(7) In the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.

SEC. 304. EFFECT OF OTHER REPORTING. An insurer shall not be considered to have satisfied the notification requirements of this Act by reporting information related to a cybersecurity incident to any person, agency or organization, including a law enforcement agency, other than to the Secretary, or to any other entity or official at the direction of the Secretary, pursuant to this Act, using the incident reporting procedures established by the Secretary.

SEC. 305. DISCLOSURE, RETENTION, AND USE.

(a) AUTHORIZED ACTIVITIES.—Cybersecurity incidents and related reporting information provided to the Secretary, or to any other entity or official at the direction of the Secretary, pursuant to this Act, may be disclosed to, retained by, or used by, any Federal agency or department, component, officer, employee, or agent of the Federal government, consistent with otherwise applicable provisions of Federal law, solely for—

(1) a cybersecurity purpose;

(2) the purpose of identifying—

(A) a cybersecurity threat, including the source of such cybersecurity threat; or

(B) a security vulnerability; or

(3) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(4) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety;

(5) the purpose of analyzing cyber insurance-related data and evaluating and managing activities under the Program or other provisions of this Act; or

(6) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in paragraph (3) or any of the offenses listed in—

(A) sections 1028 through 1030 of Title 18, United States Code (relating to fraud and identity theft);

(B) chapter 37 of such Title (relating to espionage and censorship); and

(C) chapter 90 of such Title (relating to protection of trade secrets).

(b) PROHIBITED ACTIVIES.—Cybersecurity incidents and related reporting information provided pursuant to this Act shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subsection (a).

(c) PRIVACY AND CIVIL LIBERTIES.—Cybersecurity incidents and related reporting information provided pursuant to this Act shall be retained, used, and disseminated by the Federal government—

(1) in a manner that protects from unauthorized use or disclosure to the greatest extent consistent with the purposes of this Act, any reporting information that may contain—

(A) personal information of a specific individual; or

(B) information that identifies a specific individual; and

(2) in a manner that protects the confidentiality of cybersecurity incident reporting information containing—

(A) personal information of a specific individual; or

(B) information that identifies a specific individual.

(d) FEDERAL REGULATORY AUTHORITY.—Cybersecurity incidents and related reporting provided pursuant to this Act shall not be used by any Federal, State, tribal, or local government to regulate, including by an enforcement action, the lawful activities of any non-Federal entity.

TITLE IV – CYBERATTACK ATTRIBUTION

SEC. 401. ESTABLISHMENT OF THE CYBER THREAT INTELLIGENCE INTEGRATION CENTER.

(a) ESTABLISHMENT OF CENTER.—There is established within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

(b) DIRECTOR OF CYBER THREAT INTELLIGENCE INTEGRATION CENTER.—The Cyber Threat Intelligence Integration Center shall be headed by a Director of Cyber Threat Intelligence Integration, who—

(1) shall report to the Director of National Intelligence and, when acting in support of the Secretary in carrying out section 402 of this Title, to the Secretary; and

(2) may not simultaneously serve in any other capacity in the executive branch.

(c) PRIMARY MISSIONS OF THE CENTER.—The primary missions of the Cyber Threat Intelligence Integration Center shall be as follows:

(1) Provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting United States national interests.

(2) Support the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force, United States Cyber Command, the Secretary, the National Cyber Director, the Cybersecurity Infrastructure Security Agency, and other relevant United States Government entities by providing access to intelligence necessary to carry out their respective missions.

(3) Oversee the development and implementation of intelligence sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests among the organizations referenced in subsection (b) of this section.

(4) Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence

channels are downgraded to the lowest classification practicable for distribution to both United States Government and United States private sector entities through the mechanism described in section 4 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity) and in support of attribution certifications and related public statements by the Secretary.

(5) Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

(6) Serve as the lead coordinator for the United States Intelligence Community's analytic assessment for cyber attribution and as the central and shared knowledge bank on cyber actors, as well as their goals, strategies, capabilities, and sponsoring organizations.

(7) Provide all necessary support to the Secretary, including all support required in this Title, and facilitate declassification for public release of all attribution certifications and related public statements by the Secretary.

SEC. 402. CERTIFICATION OF ATTRIBUTION FOR CATASTROPHIC CYBERATTACK INSURANCE PROGRAM PARTICIPATION

(a) PUBLIC CERTIFICATION OF ATTRIBUTION.—For any cyberattack resulting in damage within the United States, the Secretary may, and for a 'catastrophic cyberattack' certified by the Secretary under this Act, the Secretary shall, as soon as reasonably practicable, but in no event more than ninety days following such a cyberattack, in consultation with the Director of the Cyberthreat Intelligence Integration Center, National Cyber Director, and the Cybersecurity Infrastructure and Security Agency, issue a public certification of attribution.

(b) CONTENT OF CERTIFICATION OF ATTRIBUTION.—Any Certification of Attribution by the Secretary under this Title shall state, with as much supporting information as the Secretary, in consultation with the Cybersecurity Infrastructure and Security Agency, the National Cyber Director, reasonably believes should be publicly disclosed:

(1) The identity of the cyber attacker(s) primarily responsible for the attack, including whether or not the attacker is/are, or acted on behalf of, a foreign nation; or

(2) That such an identification to a reasonable certainty is not possible based on information then available to the United States. In any case in which the Secretary announces such an inability to certify an attribution, the Secretary shall specify a date, but in no event more than ninety days after such certification, by which the Secretary shall make a final certification of attribution or inability to certify attribution.

(c) PROCEDURES FOR PUBLIC CERTIFICATION OF ATTRIBUTION.—In preparing and publicly releasing any Certification of Attribution under this Title, the Secretary shall consult with the Director of the Cyberthreat Intelligence Integration Center, the National Cyber Director, the Cybersecurity Infrastructure and Security Agency, and such other officials as the Secretary shall deem appropriate.

(d) DIRECTOR OF THE CYBERTHREAT INTELLIGENCE INTEGRATION CENTER.—In fulfilling the functions of this Title, the Director of the Cyberthreat Intelligence Integration Center shall report to the Secretary, but shall keep the Director of National Intelligence fully and currently informed of activities under this Title.

(e) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—Prior to issuing any public certification of attribution, the Secretary shall consult with the Director of National Intelligence for the purpose of protecting intelligence sources and methods in any public certification of attribution.

(f) DETERMINATIONS FINAL.—Any certification of, or determination not to certify, attribution under this Title shall be final, and shall not be subject to judicial review.

(g) TIMING OF CERTIFICATION.—Not later than 9 months after the effective date of this Act, the Secretary shall issue final rules governing the process by which the Secretary shall certify an attribution under this paragraph.

(h) NONDELEGATION.—The Secretary may not delegate or designate to any other officer, employee, or person, any determination under this

paragraph of whether, during the effective period of the Program, a catastrophic cyberattack has occurred.

SEC. 403. MANDATORY ACCEPTANCE OF CERTIFICATION OF ATTRIBUTION FOR CATASTROPHIC CYBERATTACK INSURANCE PROGRAM PARTICIPATION

(a) IN GENERAL.—An insurer, in order to be eligible for the Program, must agree to accept as conclusive, and not challenge in any litigation, arbitration, or other dispute, a Certificate of Attribution for a catastrophic cyberattack under this Act.

TITLE V—NON-ENFORCEMENT OF WAR EXCLUSIONS IN CYBER INSURANCE POLICIES

SEC. 501. An insurer, in order to be eligible for the Program, shall not seek to enforce any War Exclusion, as defined in this Act, in connection with a cyberattack to deny or limit coverage or payment to an insured of an otherwise valid claim.

TITLE VI—MISCELLANEOUS

SEC. 601. CONSTITUTIONAL AVOIDANCE. The provisions of this Act shall be construed, to the greatest extent practicable, to avoid conflicting with the Constitution of the United States, including the protections established under the First Amendment to the Constitution of the United States.

SEC. 602. SEVERABILITY. If any provision of this Act, or an amendment made by this Act, is determined to be unenforceable or invalid, the remaining provisions of this Act and the amendments made by this Act shall not be affected.

SEC. 603. AUTHORIZATION OF APPROPRIATIONS. Except as otherwise indicated in this Act, there are authorized to be appropriated such sums as may be necessary to carry out this Act.

APPENDIX B: COULD IT HAPPEN?

A. THE WATER HEATERS

According to a report in *Wired* magazine, researchers at Princeton University concluded in a 2018 simulation that as few as forty-two thousand connected water heaters could be attacked by a large "botnet" to catastrophic effect.[159] The attackers could use these hijacked appliances to rapidly increase the energy demand, overloading the current on power lines and either disabling these lines or triggering emergency protective mechanisms to shut down sections of the power grid. This would then place a higher demand on other parts of the remaining lines, creating a series of cascading power blackouts. "In the worst case," said one of the researchers, "most or all of them are disconnected and you have a blackout in most of your grid."[160]

> The researchers don't actually point to any vulnerabilities in specific household devices, or suggest how exactly they might be hacked. Instead, they start from the premise that a large number of those devices could somehow be compromised and silently controlled by a hacker. That's arguably a realistic assumption, given the myriad vulnerabilities other security researchers and hackers have found in the internet of things. One talk at the Kaspersky Analyst Summit in 2016 described security flaws in air conditioners that could be used to pull off the sort of grid disturbance that the Princeton researchers describe. And real-world malicious hackers have compromised everything from refrigerators to fish tanks.
>
> Given that assumption, the researchers ran simulations in power grid software MATPOWER and Power World to determine what sort of botnet could disrupt what size grid. They ran most of their simulations on models of the Polish power grid from 2004 and 2008, a rare country-sized electrical system whose architecture is described in publicly available records. They found they could cause a cascading

---

[159] Andy Greenberg, *How Hacked Water Heaters Could Trigger Mass Blackouts*, WIRED (Aug. 13, 2018, 7:00AM), https://www.wired.com/story/water-heaters-power-grid-hack-blackout/.

[160] *Id.*

> blackout of 86 percent of the power lines in the 2008 Poland grid model with just a one percent increase in demand. That would require the equivalent of 210,000 hacked air conditioners, or 42,000 electric water heaters.[161]

B. TAKING DOWN A CLOUD INFRASTRUCTURE

At least 500 million Internet of Things (IoT) devices like these smart-home controllers are connected to the "IoT Core" of Amazon Web Services (AWS).[162] Globally, at least thirty-five *billion* such devices will come online this year, with at least *125 billion* by 2030.[163] We may assume that the relatively few cloud-hosting services, like AWS, will amass more and more of these devices, working their magic through tens of thousands of computer servers distributed around the world. [164] For obvious reasons, such companies are rich and common targets for hackers of all stripes.[165] In its 2021 *Global Threat Report*, CrowdStrike predicts:

---

[161] *Id.*

[162] Matt Kapko, *AWS Unleashes Divergent, Specialized IoT Strategy*, SDXCENTRAL (Dec. 16, 2020, 2:11 PM), https://www.sdxcentral.com/articles/news/aws-unleashes-divergent-specialized-iot-strategy/2020/12/.

[163] LEONIE MARIA TANCZER, INE STEENMANS, IRINA BRASS & MADELINE CARR, LLYOD'S OF LONDON, NETWORKED WORLD: RISKS AND OPPORTUNITIES IN THE INTERNET OF THINGS 5 (2018), https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/internet-of-things/networkedworld2018.pdf (noting that as the number of connected devices increases exponentially, so does the potential destructive power of cyberattacks utilizing such devices. As such, the ability of attackers to wreak havoc will be many orders of magnitude greater in a few years than it was last year.). *See also* Allan Jay, *Number of Internet of Things (IoT) Connected Devices Worldwide 2021/2022: Breakdowns, Growth & Predictions*, FINANCESONLINE, https://financesonline.com/number-of-internet-of-things-connected-devices/ (last visited Aug. 22, 2021).

[164] *See, e.g.*, Abraham & Schwarcz, *supra* note 8, at 39 ("[T]he vast majority of global cloud services outside China are only provided by three firms—Amazon, Microsoft, and Google.").

[165] *See, e.g.,* Brian Krebs, *What We Can Learn from the Capital One Hack*, KREBSON SECURITY (Aug. 2, 2019, 5:30 PM), https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/comment-page-1/ (discussing a 2019 attack on Capital One stealing at least 100 million consumer credit applications); Duncan Riley, *AWS mitigated a record-breaking 2.3 Tbps DDoS attack in February*, SILICONANGLE (June 17, 2020, 10:07 PM), https://siliconangle.com/2020/06/17/aws-mitigated-record-breaking-2-3-tbps-ddos-attack-february/ (discussing the

> While various Russian adversaries continue to employ malware as part of their operational toolkits, they have also increasingly sought to shortcut traditional operational workflows and focus directly on intelligence collection from third-party services used by their targets, including direct access to cloud-based network resources such as email servers. CrowdStrike Intelligence anticipates this trend is likely to continue in 2021, with previous attempts to breach single accounts via phishing campaigns making way for larger-scale operations against enterprise assets using compromised administrator credentials.[166]

AWS describes its cloud-hosting infrastructure as having "millions of active customers and tens of thousands of partners globally . . . . across virtually every industry and of every size . . . ."[167] Although AWS successfully resisted the largest known DDoS attack against it in February 2020,[168] the number of connected devices worldwide is projected to increase dramatically over the next few years.[169]

---

record-setting three-day Distributed Denial of Service (DDoS) attack in February 2020).

[166] CROWDSTRIKE, *supra* note 100, at 40.

[167] *Global Infrastructure: Why Cloud Infrastructure Matters*, AMAZON: AMAZON WEB SERVS., https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=1 (last visited Aug. 22, 2021).

[168] Catalin Cimpanu, *AWS Said It Mitigated a 2.3 Tbps DDoS Attack, the Largest Ever*, ZDNET (June 17, 2020, 9:03 AM), https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/.

[169] *Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025*, STATISTCA, https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (last visited Oct. 9, 2021). *See also* Statement of Rep. John Ratcliffe, *supra* note 4. Researchers and journalists continue to study the possibility of attack on AWS's underlying infrastructure, which would go beyond widely reported attacks on customers hosted on AWS such as Citibank and Tesla. It is unclear whether the infrastructure that supports all of AWS in an entire region could be taken offline by known hacking techniques and today's technologies. *See* Stephen Foster, *Can AWS be Hacked? – The Simple Answer*, AWS COACH, https://awscoach.net/can-aws-be-hacked/ (last visited Aug. 29, 2021). Again, the point of this study is not to prove or disprove the viability of an attack on AWS or any other cloud services provider but rather to explore the implications for the cyber insurance ecosystem of such a catastrophic attack in the future.

C. MORE ON THE POTENTIAL FOR A TRILLION-DOLLAR CYBERATTACK

Could our hypothetical water heater/AWS attack cause damage reaching into the trillions of dollars?[170] As of early 2020, Amazon boasted more than one million active users, and perhaps significantly more, with enterprise-scale users making up at least 100,000 of these.[171] Ranging from Adobe and Apple to Zillow and Zynga, AWS customers at that time also included the United States Central Intelligence Agency, Comcast, Dow Jones, Facebook, Lyft, NASA, Novartis, Pfizer, and Twitter.[172] As recently as January 2016, Netflix's use alone reportedly put sufficient stress on AWS to "push[ ] the service to its limits and beyond."[173]

According to an October 2020 report entitled *The State of the Public Cloud in the Enterprise*, seventy-seven percent of all businesses were using some degree of cloud services, with eighty-three percent of the five thousand managers surveyed stating they plan to expand their cloud adoption.[174] The same report states that nearly sixty-five percent of all businesses using the cloud use AWS.[175] A November 2020 *Techcrunch* headline read "Amazon

---

[170] A "catastrophe," in property insurance terms, has been defined as "a natural or man-made disaster that is unusually severe. An event is designated a catastrophe by the industry when claims are expected to reach a certain dollar threshold, currently set at $25 million, and more than a certain number of policyholders and insurance companies are affected." *Spotlight on: Catastrophes - Insurance Issues*, INS. INFO. INSTIT., https://www.iii.org/publications/insurance-handbook/insurance-and-disasters/spotlight-on-catastrophes-insurance-issues (last visited Aug. 22, 2021). For purposes of this paper, we are using the term "catastrophe" to mean a much larger event or set of events, with the possibility of exhausting the globally available funds for non-life insurance and reinsurance.

[171] John Cave, *Who's Using Amazon Web Services? [2020 Update],* CONTINO (Jan. 28, 2020), https://www.contino.io/insights/whos-using-aws.

[172] *Id.*; *Cloud Computing for the U.S. Intelligence Community*, AWS: GOV'T, https://aws.amazon.com/federal/us-intelligence-community/ (last visited Oct. 9, 2019). It does not take a great deal of imagination to picture the catastrophic effects, particularly during a pandemic, of taking down just a fraction of these.

[173] *Id.*

[174] MICHAEL CHALMERS & RYAN LOCKARD, CONTINO, THE STATE OF THE PUBLIC CLOUD IN THE ENTERPRISE 6–7 (2020), https://cdn.sanity.io/files/hgftikht/production/adba05d7be9df7c125953a12afdea21221095865.pdf.

[175] *Id.* at 10.

Web Services outage takes down a portion of the internet with it."[176] The incident impacted the New York City subway, Roku, and even, ironically, crippling Amazon's own service status dashboard.[177] In reporting the incident, *Forbes* noted that a similar 2017 outage "disrupted large swathes of the internet . . . ."[178]

Finally, multiple security professionals have concluded that the likely Russian – and possibly Chinese – sponsored SolarWinds attacks first detected in 2020 specifically targeted Microsoft and other cloud-based services.[179] Microsoft President Brad Smith has called SolarWinds – which reportedly struck at least eighteen thousand organizations worldwide – the "largest and most sophisticated attack ever" and concluded that the attackers had used at least one thousand engineers to decide and manage the devastating series of compromises.[180]

We can only speculate on the results if that amount and volume of expertise were directed at AWS's, or another cloud-provider's infrastructure but, to us, the breathtaking success of SolarWinds, as well as how long it took for these attacks even to be detected, makes a trillion-dollar takedown

---

[176] Zack Whittaker, *Amazon Web Services outage takes a portion of the internet down with it*, TECHCRUNCH (Nov. 25, 2020, 12:32 PM), https://techcrunch.com/2020/11/25/amazon-web-services-outage-takes-a-portion-of-the-internet-down-with-it/.

[177] Siladitya Ray, *Amazon Web Services Outrage Takes Down Major Sites Including Roku, Flickr*, FORBES (Nov. 25, 2020, 1:24 PM), https://www.forbes.com/sites/siladityaray/2020/11/25/amazon-web-services-outage-takes-down-major-sites-including-roku-flickr/?sh=393c53814291.

[178] *Id.* (noting Amazon rivals Microsoft, Google, and Alibaba combined only account for 28% of the cloud computing market, concluding that "any outage at Amazon can have a cascading impact on large swathes of the Internet."). That said, AWS's competitors also are undoubtedly targets for massive—and potentially catastrophic—cyberattacks. For example, the SolarWinds attackers "demonstrated exceptional knowledge of Microsoft O365 and the Azure environment" and their "comfort and capabilities in abusing Axure and O365 demonstrate that they have a detailed understanding of the authentication and access controls associated with these platforms." CROWDSTRIKE, *supra* note 100, at 18.

[179] Christopher Budd, *How the SolarWinds hackers are targeting cloud services in unprecedented cyberattack*, GEEKWIRE (Dec. 23, 2020, 10:45 AM), https://www.geekwire.com/2020/solarwinds-hackers-targeting-cloud-services-unprecedented-cyberattack/.

[180] Duncan Riley, *Microsoft's Brad Smith labels SolarWinds hack 'largest, most sophisticated attack ever'*, SILICONANGLE (Feb. 15, 2021, 8:57 PM), https://siliconangle.com/2021/02/15/microsofts-brad-smith-labels-solarwinds-hack-largest-sophisticated-attack-ever/.

at least plausible enough to consider the implications for the cyber insurance ecosystem.

More broadly, based on our research and analysis, a cascading series of cyberattacks across our infrastructures and economies are not the only set of circumstances that could decimate the global insurance ecosystem all of us (whether consciously or not) rely on as a final backstop to catastrophe.[181] In 2020, it was the global COVID-19 pandemic that triggered consideration of the potential for a global insurance crisis.[182] Catastrophe experts have predicted trillion-dollar hurricanes,[183] and even solar eruptions,[184] as potentially in our near future.

As Texans learned in February 2021, electric power is a fragile and precious resource and the magnitude of risk associated with potential cyberattacks on our critical infrastructure was not lost on a number of our interviewees:

> [T]he American government is yelling as quietly as possible that our grid is . . . being infected. . . . So, everybody knows that - because you already saw it in Georgia, and you saw it in the Ukraine, that the first stroke is you're going to turn out the lights on the civilian population. So, the cyber policies have war exclusions. And that's what's being litigated right now with regard to NotPetya. Zurich doesn't want to pay a

---

[181] Dave Ingram, *2020: Most Dangerous Risks to Insurers*, INT'L COOP. & MUT. INS. FED'N (Feb. 21, 2020), https://www.icmif.org/blog_articles/2020-most-dangerous-risks-to-insurers/.

[182] *See, e.g.*, Mario Chakar, Assoc., S&P Global, PowerPoint Presentation: Top Risks for the Global Insurance Industry, 3 (Nov. 17, 2020), https://www.spglobal.com/_assets/documents/ratings/research/100047463.pdf (predicting "[t]he impact of COVID-19 on global insurance markets is largely felt through asset risks, notably capital markets volatility, and weaker premium growth prospects."); Laura J. Hay, *Do insurers have COVID-19 covered?*, KPMG INT'L, https://home.kpmg/xx/en/home/insights/2020/03/do-insurers-have-covid-19-covered.html (last visited Aug. 22, 2021) (stating that market volatility will likely impact insurers).

[183] Greg Lindsay, *The Trillion-Dollar Storm: Will Hurricanes Drive Us Off The Coasts?*, FAST COMPANY: BUTTERFLY EFFECT (Oct. 4, 2011), https://www.fastcompany.com/1783816/trillion-dollar-storm-will-hurricanes-drive-us-coasts.

[184] Marshall Shepherd, *A Trillion Dollar Storm Looms For Earth And It's Not A Hurricane*, FORBES (Oct. 10, 2019, 8:11 AM) (citing Robert Coker, *The trillion-dollar (solar) storm*, SPACE REV. (Oct. 30, 2017), https://www.thespacereview.com/article/3358/1), https://www.forbes.com/sites/marshallshepherd/2019/10/10/a-trillion-dollar-storm-looms-for-earth-and-its-not-a-hurricane/?sh=eb216136ebcc.

> very large . . . claim by a candy manufacturer in Chicago [Mondelez], because they say that NotPetya was an act of war because there's a war exclusion. So, with regard to Azure [large cloud service provider] . . . *the domestic insurers are just praying*.[185]

One could even imagine an opportunistic nation-state or other hackers taking advantage of a pandemic to launch a crippling cyberattack on virus development or deployment by their enemies[186] and *combining it* with one or more other critical infrastructure cyberattacks.

---

[185] Zoom Interview with Risk Manager & Underwriter, *supra* note 1.

[186] *See* CROWDSTRIKE, *supra* note 100, at 12 tbl.1 (noting China, Iran, North Korea, Russia, and Vietnam, as well as nongovernmental cyber-crime groups, all likely targeted the healthcare sector or the governments' responses to the COVID-19 pandemic in 2020).